



TITELSTORY

GROSSPROJEKT «SEDH»

**Der «Swiss Emergency Data Hub»
vernetzt Einsatzkräfte bei kooperativen
Ereignissen – über Organisations-
und Einsatzraumgrenzen hinweg**

**RÜCKLICHT
FACHTAGUNG PSNV
NEUES ZUR PSYCHOSOZIALEN
NOTFALLVERSORGUNG
IN DER SCHWEIZ**



TEST & TECHNIK DAS HANDY ALS BARGELDSCANNER

OVD Kinegram entwickelt App
«BANKNOTE SCANNER»

FOKUS AUF DEN SPUREN DES BARGELDS

Inkriminierte Banknoten nachverfolgen –
durch Seriennummern-Tracking

EVENTS SPIK 2026

Grosse Vorschau auf den
Schweizer Polizei Informatik Kongress
mit MSK-Halbtage in Bern

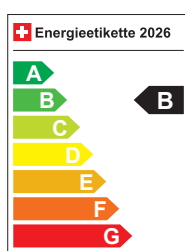


Der neue Volvo EX60

Der neue Volvo verbindet eine Reichweite von bis zu 810 km mit schneller Ladeleistung: In nur 10 Minuten lädst du unterwegs bis zu 340 km nach. Der Innenraum überzeugt mit grosszügigem Interieur und ergonomischen Sitzen, die für besonderen Komfort sorgen – ganz gleich, wie lang deine Reise ist.

Freedom to move. Electric.

volvocars.ch/EX60



Volvo EX60 P12 AWD, 680 PS/500 kW.
Stromverbrauch gesamt: 16 kWh/100 km,
CO₂-Emissionen: 0 g/km.
Energieeffizienz-Kategorie: B.

VOLVO





zuverlässige Verbindungen für Blaulicht Organisationen



Unsere Technologien



4G/5G Mobilfunk

Extrem schnelle Datenübertragung, geringe Latenz und hohe Verbindungsdichte. Ideal für IoT, autonome Fahrzeuge und smarte Städte.



Starlink Satelliteninternetdienst

Garantiert schnelles Internet weltweit, auch in abgelegenen Gebieten und unterwegs.



SPEEDFUSION

Bandwith Bonding

Peplink Bonding kombiniert mehrere Internetverbindungen (z.B. Mobilfunk, Starlink, usw.) zu einer schnellen, stabilen, ausfallsicheren und verschlüsselten Verbindung.



www.smaro.ch

Besuchen Sie uns an der SPIK 2026
Sehen Sie unsere Anwendungsfälle mit Mobile 5G und Starlink

www.peplink.com



www.spik.ch

» GRENZEN ÜBERWINDEN
» DÉPASSER LES FRONTIÈRES
» SUPERARE I CONFINI



» Dr. Jörg Rothweiler

Liebe Leserschaft!

» Gemeinsamkeit macht stark! Denn sie ist ein Überlebensfaktor, der hilft, Krisen besser zu überstehen: Bündeln Individuen ihre Kräfte, Talente und Ressourcen, wird möglich, was Einzelne nicht schaffen. Sie selbst erleben diese Kraft der Synergie immer wieder. Wenn Sie Ereignisse bewältigen, kooperativ, Hand in Hand mit Dritten.

Da Grenzen Synergien zerstören, ist das Potenzial des Projekts «Swiss Emergency Data Hub» enorm. Weil dieses Grenzen abbaut – mithilfe digitaler Methoden.

Dasselbe, wenngleich auf ganz anderer Ebene, leistet eine Lösung der Elephant & Castle IP GmbH. Diese ermöglicht es, inkriminierte Geldscheine nachzuverfolgen – was die Möglichkeiten der Strafverfolgung potenziert.

Grenzen neu definiert werden auch beim Schweizer Polizei Informatik Kongress SPIK, der 2026 noch grösser wird. Alles Wissenswerte dazu lesen Sie bei uns.

Und wenn menschliche Grenzen überschritten wurden, schlägt die Stunde der Fachkräfte der psychologischen und psychosozialen Notfallversorgung. Was in diesem Bereich neu ist, erfahren Sie bei der 12. Fachtagung der Schweizerischen Vereinigung für Psychosoziale Notfallversorgung. Auch hierzu liefern wir alle Informationen.

Ich wünsche der gesamten BORS-Gemeinschaft eine spannende Lektüre!

Dr. Jörg Rothweiler, Chefredakteur
j.rothweiler@blaulicht-iv.ch

Cher lectorat,

» L'union fait la force ! C'est en effet un facteur de survie qui aide à mieux surmonter les crises : lorsque des individus unissent leurs forces, leurs talents et leurs ressources, ils peuvent accomplir ce qu'ils ne pourraient réaliser seuls. Vous-même faites régulièrement l'expérience de cette force de synergie. Lorsque vous surmontez des événements, en coopération, main dans la main avec des tiers.

Comme les frontières détruisent les synergies, le potentiel du projet « Swiss Emergency Data Hub » est considérable. Car il abolit les frontières à l'aide de méthodes numériques.

C'est ce que fait également une solution proposée par Elephant & Castle IP GmbH, bien qu'à un tout autre niveau. Elle permet de tracer les billets de banque incriminés, ce qui multiplie les possibilités de poursuites pénales.

Les frontières sont également redéfinies lors du Congrès suisse sur l'informatique policière SPIK, qui sera encore plus grand en 2026. Vous trouverez toutes les informations utiles à ce sujet dans cette édition.

Et lorsque les limites humaines sont dépassées, c'est au tour des spécialistes de l'aide psychologique et psychosociale d'urgence d'intervenir. Vous découvrirez les nouveautés dans ce domaine lors du 12^e colloque de la Schweizerische Vereinigung für Psychosoziale Notfallversorgung. Nous vous dévoilons également toutes les informations à ce sujet.

Je souhaite à toute la communauté des AOSS une lecture passionnante!

Dr. Jörg Rothweiler, Rédacteur en chef
j.rothweiler@blaulicht-iv.ch

Gentili lettori,

» l'unione fa la forza! Essa garantisce sopravvivenza e aiuta a superare le crisi: quando le persone uniscono le loro forze, i loro talenti e le risorse a che hanno a disposizione, riescono a fare cose che un singolo non potrebbe mai portare a termine. Anche voi e sperite di continuo la forza di questa sinergia quando affrontate degli eventi in stretta cooperazione con terzi.

Dato che i confini compromettono le sinergie, il potenziale del progetto «Swiss Emergency Data Hub» è enorme. Lo è proprio perché abbatte i confini con l'aiuto di metodi digitali.

Un contributo simile, seppur su un piano completamente diverso, è dato dalla soluzione di Elephant & Castle IP GmbH. Questa permette di tracciare banconote incriminate, potenziando le possibilità di perseguimento penale.

Una nuova ridefinizione dei confini viene poi data al Congresso di informatica della Polizia svizzera (SPIK), che nel 2026 sarà ancora più grande. Potrete saperne di più leggendo questo numero.

Quando poi sono i confini umani ad essere oltrepassati, è bene affidarsi agli esperti dell'aiuto psicologico e psicosociale d'urgenza. Le novità del settore saranno presentate al 12. Convegno dell'Associazione Svizzera per l'aiuto psicosociale d'urgenza (PSNV). Anche su questo tema vi forniamo tutte le informazioni utili.

All'intera comunità delle AOSS auguro una piacevole lettura!

Dr. Jörg Rothweiler, Caporedattore
j.rothweiler@blaulicht-iv.ch

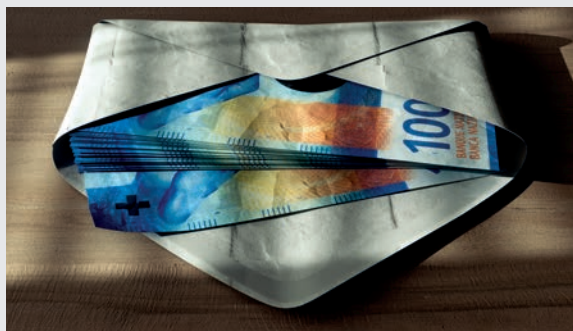


Rega

» TITELSTORY » THEME PRINCIPAL

» TEMA PRINCIPALE

- 13 » Demokratisierung des Rettungswesens:
Das Projekt «Swiss Emergency Data Hub» (SEDH)
- 17 » Démocratisation des services de secours :
Le projet « Swiss Emergency Data Hub » (SEDH)
- 22 » Democratizzazione del salvataggio:
il progetto «Swiss Emergency Data Hub» (SEDH)



shutterstock.com

» FOKUS » FOCUS » FOCUS

- 27 » Bargeldtracking:
Auf den Spuren inkriminierter Geldscheine
- 31 » Suivi des espèces :
Sur les traces des billets suspects
- 35 » Tracciamento dei contanti:
Sulle tracce dei biglietti incriminati



zVg

» EVENTS » NUMÉRISATION » DIGITALIZZAZIONE

- 43 » Vorschau auf den SPIK 2026 in Bern
- 46 » Aperçu du SPIK 2026 à Berne
- 49 » Anteprima dello SPIK 2026 a Berna



Die sicherste Alarmübermittlung der Schweiz
La transmission d'alarme la plus sûre de Suisse
La trasmissione di allarme più sicura della Svizzera

» TEST & TECHNIK » TEST & TECHNIQUE

» TEST & TECNICA

- 52 » «BANKNOTE SCANNER» von OVD Kinegram:
Banknoten im mobilen Einsatz identifizieren
und dokumentieren – schnell und sicher
- 54 » « BANKNOTE SCANNER » d'OVD Kinegram AG :
Identifier et documenter les billets de banque
lors d'une intervention mobile, rapidement
et en toute sécurité
- 56 » «BANKNOTE SCANNER» di OVD Kinegram AG:
Identificare e documentare le banconote nelle
operazioni mobili in modo rapido e sicuro

» MITTEL & METHODEN » MOYENS ET MÉTHODES

» MEZZI & METODI

- 59 » Forum Innere Sicherheit 2025 des VSPB:
Künstliche Intelligenz im Polizeieinsatz –
Segen oder Risiko?
- 63 » Forum sur la Sécurité intérieure 2025 de la FSFP :
L'intelligence artificielle dans les services de police –
bénédiction ou risque ?
- 67 » Forum Sicurezza Interna 2025 della FSFP:
Intelligenza artificiale al servizio di polizia –
una benedizione o un rischio?

» RÜCKLICHT » FEU ARRIÈRE » LUCE POSTERIORE

- 72 » 12. Fachtagung PSNV am 9. Mai 2026 in Sursee:
Neues zur psychosozialen Notfallversorgung
- 74 » 12^e Colloque PSNV le 9 mai 2026 au Campus Sursee :
Actualités concernant la prise en charge
psychosociale d'urgence
- 76 » 12. Convegno PSNV in data 9 maggio 2026:
Nuovi sviluppi nell'aiuto psicosociale d'urgenza

» SERVICE » SERVICE » SERVIZIO

- 78 » Vorschau, Agenda und Impressum
- 78 » Aperçu, agenda et mentions légales
- 78 » Anteprima, agenda e impronta

» NEWS | » NOUVELLES » NOTIZIE

- 4 » ■ sureVIVE offizieller Sponsor von Seilbahnen Schweiz
 - Mobilität: neuer Volvo EX60 mit 810 km Reichweite
 - Berner IT-Projekt «Nevo/Rialto» wird beendet
 - Mobiles Arbeiten: Panasonic TOUGHBOOK mit Akku-Innovationen und KI
 - IT-Markt: CONVOTIS schärft strategischen Fokus
- 6 » ■ sureVIVE devient sponsor officiel de Remontées Mécaniques Suisses
 - Mobilité : Volvo EX60 avec 810 km d'autonomie
 - Le projet informatique bernois « Nevo/Rialto » se termine
 - Travail mobile : Panasonic TOUGHBOOK avec des innovations en matière de batterie et d'IA
 - CONVOTIS affine son orientation stratégique
- 8 » ■ sureVIVE ora sponsor ufficiale di Funivie Svizzere
 - Volvo EX60 con una portata di 810 chilometri
 - Il progetto informatico di Berna «Nevo/Rialto» viene terminato
 - MOBILE WORKING: Panasonic TOUGHBOOK con innovazioni a batteria e IA
 - CONVOTIS affina l'attenzione sulla strategia

Swisscom Broadcast AG

WEF Davos:

Wenn der Blick nach oben Teil
der Einsatzführung wird

10

WEF Davos:

Quand la surveillance aérienne s'intègre
pleinement à la conduite des interventions

11

Computacenter AG

Technologie, die Sicherheit stärkt.

IT-Kompetenz für Blaulichtorganisationen

26

JORLAR s.r.o.

TachoScan Control

Präzise und effiziente Kontrolle
von Lenk- und Ruhezeiten

41

om computer support ag

/om News

Innovative Lösungen

für die öffentliche Sicherheit

58



Arosa
Gemeinde

GEMEINDE AROSA SUCHT

ab 1. März 2026 oder nach Vereinbarung
einen Polizisten/eine Polizistin

**STELLENANZEIGE UND WEITERE
INFORMATIONEN FINDEN SIE
AUF DER SEITE 70**



GENDERHINWEIS:

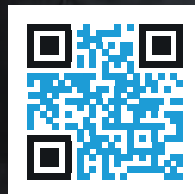
Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsneutrale Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter. Die verkürzte Sprachform beinhaltet keine Wertung.



printed in
switzerland

MAXIMAL FUNKTIONAL IM DIENST

EINSATZSTIEFEL AUS LEDER MIT
ZUSÄTZLICHEM SPITZENSCHUTZ



JETZT ENTDECKEN



BLACK EAGLE®
TACTICAL PRO 2.1 GTX MID



HAIX Switzerland

HAIX® Vertriebs AG | Bielgraben 1 | 4622 Egerkingen | haix.ch

RETTUNG

» sureVIVE jetzt offizieller Sponsor von Seilbahnen Schweiz

Das auf Alarmierungs- und Einsatzführungssysteme spezialisierte Software-Unternehmen sureVIVE AG aus Mendrisio hat die etablierte Zusammenarbeit mit dem Verband der Schweizer Seilbahnbranche «Seilbahnen Schweiz SBS» auf eine neue strategische Ebene gehievt: Seit Ende 2025 tritt sureVIVE als offizieller Sponsor von SBS auf – basierend auf der bestehenden Rolle als Industriepartner. Inhaltlich zielt der Vertrag laut sureVIVE darauf ab, das Bergbahnpersonal sowie die Pisten- und Rettungsdienste bei Unfällen und Evakuationen digital zu unterstützen. Ein besonderer Fokus liegt auf der digitalen Integration in die Rettungskette – im Sinne der Vision «Rettung Schweiz 2034» des Interverbands für Rettungswesen (IVR) – sowie auf der Optimierung von Abläufen bei Bergbahnrettungen durch technische Innovation und operative Vernetzung.

Die sureVIVE AG ist in der Blaulichtwelt bekannt für die in 22 Kantonen genutzte First-Responder-App «Momentum», das flexible Alarmierungs- und Einsatzführungssystem «Momentum PRO» sowie «Momentum EYE», eine Live-Video-Lösung für Rettungskräfte. Die Branchenvertretung Seilbahnen Schweiz (SBS) hat rund 350 ordentliche Mitglieder aus allen Regionen des Landes, vertritt die gemeinsamen Anliegen und Interessen der Mitglieder und fördert ihre Zusammenarbeit. Zu den Aufgaben von SBS gehören auch die Ausbildung von Mitarbeitenden im Pisten- und Rettungsdienst (u. a. im Ausbildungszentrum Meiringen) und die Sicherstellung der Verkehrssicherungspflicht auf den Pisten und Sommeranlagen der Seilbahnunternehmen.

Mehr Informationen finden Interessierte auf: www.surevive.ch

MOBILITÄT

» Vollelektrischer Volvo EX60 mit 810 km Reichweite

Mitte Januar liess Volvo die Katze aus dem Sack: Die bei BORS seit Jahren beliebten Modelle EX60 und EX60 «Cross Country» kommen neu vollelektrisch – mit bis zu 810 Kilometer Reichweite (WLTP-Standard kombiniert), maximal 680 PS Leistung und optionalem Allradantrieb.

Die Basis markiert der EX60 P6 mit Heckantrieb, 374 PS, 83-kWh-Akku und 620 bis 740 Kilometer Reichweite (kombiniert/innerorts). Allrad gibt es ab dem Modell EX60 P10, das 510 PS leistet und dank 95-kWh-Akku 660 bis 790 Kilometer weit stromert. Das Topmodell EX60 P12 glänzt mit 117-kWh-Akku, Allradantrieb, 680 PS und stattlichen 810 bis 980 Kilometer Reichweite.

Das Laden von 10 auf 80 Prozent am DC-Schnelllader dauert bei allen Modellen keine 20 Minuten, wobei der EX60 P6 mit maximal 300 kW, die Allradmodelle mit bis zu 400 kW geladen werden können. An der heimischen Wallbox (AC-Lader) bunkert der EX60 mit bis zu 22 kW Energie – und bidirektionales Laden beherrscht er ebenfalls.

Mit 4,80 Meter Länge, 1,90 Meter Breite und 1,64 Meter Höhe ist der EX60 zwar gross – aber wendig genug auch für den City-Einsatz. So bietet er bis zu 5 Personen ordentlich viel Raum und einen Kofferraum, der 634 Liter fasst. Legt man die Rücksitze um, wächst der Stauraum auf maximal 1'647 Liter. Der vorne platzierte «Frunk» fasst 58 Liter.

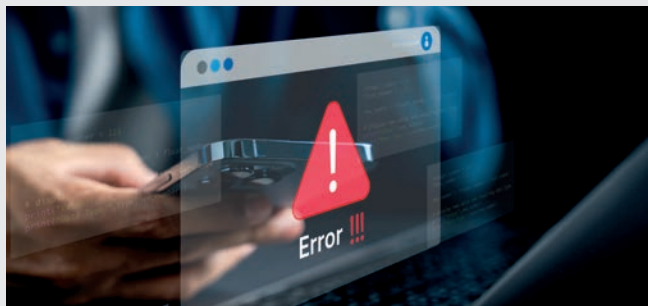
Die Preise für den EX60 starten bei 72'000 Franken für die Basisversion. Wählt man das Topmodell EX60 P12 und packt alles rein, was Volvo anbietet, werden rund 99'300 Franken fällig.

Etwas teurer wird die erst ab Mitte 2027 erhältliche «Cross-Country»-Variante mit mehr Bodenfreiheit und adaptiver Luftfederung. Diese startet ab 77'700 Franken.

Mehr Informationen erhalten Interessierte auf: www.volvocars.com/de-ch



SCHWEIZER IT-PROJEKTE

» **Berner IT-Projekt
«Nevo/Rialto» wird beendet**

Das Informatikprojekt «Nevo/Rialto» der Berner Kantonspolizei und Justiz ist endgültig gescheitert. Die Staatsanwaltschaft zog sich Ende Dezember 2025 aus dem Projekt zurück. Einerseits, weil die ursprünglich geplante digitale Datenbrücke zwischen Polizei und Justiz nie realisiert wurde. Andererseits, weil die Lieferanten Swisscom und Deloitte schon im August 2025 mitgeteilt hatten, dass die der Plattform zugrunde liegende SAP-Version ab 2031 wohl nicht mehr unterstützt wird.

Das 2015/2016 gestartete Projekt war ehrgeizig, innovativ – aber nur teilweise erfolgreich. Der Start verlief holprig, mit unzufriedenen Nutzern, Verzögerungen und Mehrkosten. Dann gab es aber doch Fortschritte. Seit 2022 nutzt die Berner Kantonspolizei «Rialto» mit zufriedenstellenden Ergebnissen – und wird es wohl bis 2031 weiter tun. Ob danach auf eine neue SAP-Version oder ein anderes System migriert werden soll, wird derzeit geprüft. Ein Entscheid soll bis Mitte 2026 fallen.

Das Projekt, anfangs budgetiert mit 13,5 Millionen Franken, kostete laut Kanton Bern bislang rund 23 Millionen Franken. Einen einstelligen Millionenbetrag soll der Kanton nun zurückerhalten – als Erstattungszahlungen oder in Form von Leistungen.

MOBILE WORKING

» **Panasonic TOUGHBOOK
mit Akku-Innovationen und KI**» **Die aktuellen Tablets und Notebooks von Panasonic TOUGHBOOK**

Panasonic erachtet leistungsstärkere Akkus, natürliche Sprachsteuerung sowie KI und 5G-Konnektivität als zentrale Technologietrends für die kommenden Generationen seiner TOUGHBOOKS. Einerseits führten längere Laufzeiten und kürzere Ladeintervalle zu höherer Einsatzverfügbarkeit. Andererseits würde eine verbesserte Sprachsteuerung eine zuverlässige, freihändige Bedienung selbst in lauten oder herausfordernden Umgebungen ermöglichen. So könnten sich Einsatzkräfte auf ihre Aufgaben konzentrieren, während das Gerät Informationen bereitstellt, Prozesse unterstützt oder kontextbezogene Hinweise liefert. Dies verbessere sowohl die Effizienz als auch die Arbeitssicherheit.

Weitere Trends seien KI und 5G-Konnektivität. Dank intelligenter Datenverarbeitung in Echtzeit, vernetzten Anwendungen und adaptiven Assistenzfunktionen sollen robuste mobile Endgeräte die Einsatzkräfte noch besser im Arbeitsalltag unterstützen. Parallel will sich Panasonic noch stärker vom Geräteanbieter zum effizienten Mobilitätspartner der Blau- und Gelblichkräfte entwickeln.

Mehr Informationen finden Interessierte auf:
<https://eu.connect.panasonic.com/de/de>

DIGITALISIERUNG

» **CONVOTIS schärft strategischen Fokus**

CONVOTIS

Die CONVOTIS Group, ein europäischer Anbieter für digitale Transformation, Cloud- und KI-basierte Lösungen, hat im Rahmen ihrer strategischen Weiterentwicklung ihre SAP Business Unit veräussert. Stattdessen soll der Fokus künftig auf vier zentralen Technologiebereichen liegen, in denen Investitionen, Innovationsaktivitäten und Managementkapazitäten gebündelt werden: digitale Transformation und KI-basierte Lösungen für Unternehmen und öffentliche Institutionen; souveräne Cloud- und Plattformlösungen mit Fokus auf europäische Datenhoheit und Compliance; Cyber Security, Cloud Security und Managed Security Services; branchenorientierte Plattform- und Managed-Services-Modelle.

In der Schweiz ist die Gruppe mit der 2023 aus der JMC Software AG hervorgegangenen CONVOTIS Schweiz AG mit Sitz in Rotkreuz im Markt aktiv – und seither auf Expansionskurs. 2023 übernahm sie die Sowatec AG (Pfäffikon ZH) und das KI-Start-up InnoFind GmbH, 2024 die Berner AGENTIL sowie die swiss cloud computing ag (Zürich) und 2025 die aspectra AG (Zürich; neu: CONVOTIS Swiss Cloud AG). Zudem besteht seit 2024 eine strategische Partnerschaft mit der Diso AG (Bern), einer Tochtergesellschaft der Securize IT Solutions AG (München).

Mehr Informationen finden Interessierte auf:
www.convotis.ch

SAUVETAGE

» sureVIVE devient le sponsor officiel de Remontées Mécaniques Suisses

L'entreprise de logiciels sureVIVE AG, basée à Mendrisio et spécialisée dans les systèmes d'alerte et de gestion des interventions, a élevé sa collaboration bien établie avec l'association suisse des remontées mécaniques « Remontées Mécaniques Suisses RMS » à un nouveau niveau stratégique : depuis fin 2025, sureVIVE est le sponsor officiel de RMS, sur la base de son rôle actuel de partenaire industriel. Selon sureVIVE, l'accord vise à fournir un soutien numérique au personnel des remontées mécaniques ainsi qu'aux services des pistes et de secours en cas d'accidents et d'évacuations. L'accent est mis en particulier sur l'intégration numérique dans la chaîne de sauvetage, conformément à la vision « Rettung Schweiz 2034 » de l'Interassociation de sauvetage (IAS), ainsi que sur l'optimisation des processus de sauvetage en montagne grâce à l'innovation technique et à la mise en réseau opérationnelle.

L'entreprise sureVIVE AG est connue dans le monde des services d'urgence pour son application « Momentum » destinée aux premiers répondants, utilisée dans 22 cantons, pour son système flexible d'alerte et de gestion des interventions « Momentum PRO » et pour « Momentum EYE », une solution de vidéo en direct pour les services de secours. L'association de la branche des remontées mécaniques suisses (RMS) compte environ 350 membres ordinaires issus de toutes les régions du pays, défend les préoccupations et les intérêts communs de ses membres et encourage leur collaboration. Parmi les missions de RMS figurent également la formation des collaborateurs des services des pistes et de secours (notamment au centre de formation de Meiringen) et la garantie de la sécurité sur les pistes et les installations estivales des entreprises de remontées mécaniques.

Retrouvez plus d'informations sur : www.surevive.ch

MOBILITÉ

» Volvo EX60 entièrement électrique avec une autonomie de 810 km

Volvo a dévoilé son projet à la mi-janvier : les modèles EX60 et EX60 « Cross Country », très appréciés depuis des années chez les AOSS, sont désormais disponibles en version entièrement électrique, avec une autonomie pouvant atteindre 810 kilomètres (norme WLTP combinée), une puissance maximale de 680 ch et une transmission intégrale en option.

L'EX60 P6 avec propulsion arrière, 374 ch, batterie de 83 kWh et une autonomie de 620 à 740 km (combinée/en ville) sert de modèle de base. La transmission intégrale est disponible à partir du modèle EX60 P10, qui développe 510 ch et offre une autonomie de 660 à 790 kilomètres grâce à sa batterie de 95 kWh. Le modèle haut de gamme EX60 P12 se distingue par une batterie de 117 kWh, une transmission intégrale, une puissance de 680 ch et une autonomie impressionnante de 810 à 980 kilomètres.

La recharge de 10 à 80 pour cent sur un chargeur rapide DC prend moins de 20 minutes pour l'ensemble des modèles, l'EX60 P6 pouvant être rechargé à une puissance maximale de 300 kW et les modèles à transmission intégrale jusqu'à 400 kW. Sur une borne de recharge domestique (chargeur AC), l'EX60 peut stocker jusqu'à 22 kW d'énergie et est également compatible avec la recharge bidirectionnelle.

Avec une longueur de 4,80 mètres, une largeur de 1,90 mètres et une hauteur de 1,64 mètres, l'EX60 est certes imposant, mais suffisamment maniable pour une utilisation en ville. Il offre ainsi suffisamment d'espace pour accueillir jusqu'à 5 personnes et dispose d'un coffre d'une capacité de 634 litres. En rabattant les sièges arrière, la capacité maximale de l'espace de rangement passe à 1 647 litres. Le « frunk » situé à l'avant offre une capacité de 58 litres.

Le prix de départ de l'EX60 est de 72 000 francs suisses pour la version de base. Si l'on opte pour le modèle haut de gamme EX60 P12 et que l'on ajoute toutes les options proposées par Volvo, il faut compter environ 99 300 francs suisses.

La version « Cross Country », qui ne sera disponible qu'à partir de mi-2027, avec une garde au sol plus importante et une suspension pneumatique adaptative, sera légèrement plus onéreuse. Son prix de départ est de 77 700 francs suisses.

Retrouvez plus d'informations sur : www.volvocars.com/fr-ch



PROJETS INFORMATIQUES SUISSES

» Le projet informatique bernois
« Nevo/Rialto » se termine

Le projet informatique « Nevo/Rialto » de la police cantonale et de la justice bernoises a définitivement échoué. Le ministère public s'est retiré du projet fin décembre 2025. D'une part, parce que

la passerelle numérique initialement prévue entre la police et la justice n'a jamais été mise en place. D'autre part, parce que les fournisseurs Swisscom et Deloitte avaient déjà annoncé en août 2025 que la version SAP sur laquelle reposait la plateforme ne serait probablement plus prise en charge à partir de 2031.

Lancé en 2015-2016, le projet était ambitieux et innovant, mais n'a connu qu'un succès partiel. Le démarrage a été compliqué, avec des utilisateurs insatisfaits, des retards et des coûts supplémentaires. Mais des améliorations ont ensuite été apportées. Depuis 2022, la police cantonale bernoise utilise « Rialto » avec des résultats satisfaisants et devrait continuer à le faire jusqu'en 2031. La question de savoir s'il convient ensuite de migrer vers une nouvelle version SAP ou vers un autre système est actuellement étudiée. Une décision devrait être prise d'ici mi-2026.

Le projet, initialement budgétisé à 13,5 millions de francs suisses, a coûté jusqu'à présent environ 23 millions de francs selon le canton de Berne. Le canton devrait désormais récupérer un montant de plusieurs millions de francs, sous forme de remboursements ou de prestations.

TRAVAIL MOBILE

» Panasonic TOUGHBOOK avec des innovations en matière de batterie et d'IA



» Les notebook robustes actuels de Panasonic TOUGHBOOK

Selon Panasonic, des batteries plus puissantes, la commande vocale naturelle, l'IA et la connectivité 5G sont des tendances technologiques essentielles pour les prochaines générations de ses TOUGHBOOK. D'une part, des durées de fonctionnement plus

longues et des intervalles de recharge plus courts entraîneraient une plus grande disponibilité opérationnelle. D'autre part, une commande vocale améliorée permettrait une utilisation fiable et mains libres, même dans des environnements bruyants ou complexes. Les forces d'intervention pourraient ainsi se concentrer sur leurs missions tandis que l'appareil fournirait des informations, assisterait les processus ou donnerait des indications contextuelles. Cela améliorerait à la fois l'efficacité et la sécurité au travail.

L'IA et la connectivité 5G constituent d'autres tendances. Grâce au traitement intelligent des données en temps réel, aux applications en réseau et aux fonctions d'assistance adaptatives, les terminaux mobiles robustes devraient encore mieux assister les forces d'intervention dans leur travail quotidien. En parallèle, Panasonic souhaite poursuivre son évolution, passant du statut de fournisseur d'appareils à celui de partenaire de mobilité efficace pour les forces d'intervention.

Retrouvez plus d'informations sur :

<https://eu.connect.panasonic.com/de/de>

fabricant

NUMÉRISATION

» CONVOTIS affine son orientation stratégique

CONVOTIS

Le groupe CONVOTIS, fournisseur européen de solutions de transformation numérique, de cloud et d'intelligence artificielle, a cédé son unité commerciale SAP dans le cadre de son développement stratégique. À l'avenir, l'accent sera mis sur quatre domaines technologiques clés, dans lesquels les investissements, les activités d'innovation et les capacités de gestion seront regroupés : transformation numérique et solutions basées sur l'intelligence artificielle pour les entreprises et les institutions publiques ; solutions cloud et de plateformes souveraines axées sur la souveraineté des données et la conformité européennes ; cybersécurité, sécurité cloud et services de sécurité gérés ; modèles de plateformes et de services gérés orientés vers l'industrie.

En Suisse, le groupe est présent sur le marché depuis 2023 avec CONVOTIS Schweiz AG, issue de JMC Software AG et basée à Rotkreuz, et poursuit depuis son expansion. Il a racheté en 2023 Sowatec AG (Pfäffikon ZH) et la start-up d'IA Innofind GmbH, en 2024 la société bernoise AGENTIL ainsi que Swiss Cloud Computing AG (Zurich) et en 2025 aspectra AG (Zurich ; désormais CONVOTIS Swiss Cloud AG). Un partenariat stratégique a en outre été conclu en 2024 avec Diso AG (Berne), une filiale de Securize IT Solutions AG (Munich).

Retrouvez plus d'informations sur : www.convotis.ch

SALVATAGGIO

» **sureVIVE ora sponsor ufficiale di Funivie Svizzere**

sureVIVE AG, la società di software specializzata nei sistemi di allarme e gestione degli incidenti con sede a Mendrisio, ha elevato la già consolidata collaborazione con l'Associazione del settore funivie svizzere «Funivie Svizzera SBS» ad un nuovo livello strategico: dalla fine del 2025, sureVIVE figura come sponsor ufficiale di SBS, basandosi sul suo precedente ruolo di partner dell'industria. In termini di contenuto, a detta di sureVIVE, il contratto ha la finalità di sostenere in modalità digitale il personale dell'impianto di risalita e i servizi sulle piste e di salvataggio in caso di incidenti ed evacuazioni. Un punto focale è l'integrazione digitale nella catena di salvataggio, in conformità alla «Visione del sistema di soccorso svizzero 2034» dell'Interassociazione di salvataggio (IAS), nonché l'ottimizzazione dei processi durante i salvataggi negli impianti di risalita, grazie a innovazioni tecniche e alla creazione di una rete operativa.

La sureVIVE AG è nota nel mondo a girofaro blu per l'app First Responder utilizzata in 22 cantoni, «Momentum», il flessibile sistema di allarme e controllo operativo «Momentum PRO» e per «Momentum EYE», una soluzione video live per le forze di salvataggio. La rappresentanza di categoria Funivie Svizzere (SBS) presenta circa 350 membri ordinari provenienti da tutte le regioni del Paese, rappresenta le questioni e gli interessi comuni a tutti i membri e favorisce la collaborazione tra di loro. I compiti della SBS includono anche la formazione dei collaboratori operanti nel servizio sulle piste e di salvataggio (anche nel Centro di formazione Meiringen) e la garanzia del rispetto degli obblighi di sicurezza stradale sulle piste e sugli impianti estivi delle società funiviarie.

Chi è interessato potrà reperire ulteriori informazioni su: www.surevive.ch

MOBILITÀ

» **Volvo completamente elettrica EX60 con una portata di 810 chilometri**

A metà gennaio, Volvo ha vuotato il sacco: i modelli EX60 ed EX60 «Cross Country», apprezzati dalle AOSS da anni, sono ora disponibili come veicoli completamente elettrici, con autonomia fino a 810 chilometri (ciclo combinato WLTP), una potenza massima di 680 CV e trazione integrale opzionale.

Il modello base è l'EX60 P6 con trazione posteriore, 374 CV, batteria da 83 kWh e un'autonomia da 620 a 740 chilometri (ciclo combinato/urbano). La trazione integrale è disponibile a partire dall'EX60 P10, con 510 CV che, grazie alla batteria da 95 kWh, raggiunge un'autonomia da 660 a 790 chilometri. Il modello top di gamma EX60 P12 vanta una batteria da 117 kWh, trazione integrale, 680 CV e un'autonomia impressionante da 810 a 980 chilometri.

La ricarica dal 10 all'80 per cento con una stazione di ricarica rapida a corrente continua richiede meno di 20 minuti per tutti i modelli, con l'EX60 P6 in grado di ricaricare fino a 300 kW e i modelli a trazione integrale fino a 400 kW. Con una wallbox domestica (caricabatterie a corrente alternata), l'EX60 può ricaricare fino a 22 kW e supporta anche la ricarica bidirezionale.

Con una lunghezza di 4,80 metri, una larghezza di 1,90 metri e un'altezza di 1,64 metri, l'EX60 è spaziosa, ma sufficientemente agile per la guida in città. Offre ampio spazio per un massimo di cinque persone e un bagagliaio con una capacità di 634 litri. Ripiegando i sedili posteriori, il vano di carico aumenta fino a un massimo di 1'647 litri. Il «Frunk» anteriore ha una capacità di 58 litri.

I prezzi dell'EX60 partono da 72'000 franchi svizzeri per il modello base. Scegliendo il modello top di gamma EX60 P12 e aggiungendo tutti gli optional offerti da Volvo, si arriva a spendere circa 99'300 franchi svizzeri.

La variante «Cross Country», disponibile a partire da metà 2027, sarà leggermente più costosa, con una maggiore altezza da terra e sospensioni pneumatiche adattive. Questa versione parte da 77'700 franchi svizzeri.

Chi è interessato potrà reperire ulteriori informazioni su: www.volvocars.com/it-ch



PROGETTI INFORMATICI SVIZZERI

» Il progetto informatico di Berna «Nevo/Rialto» viene terminato



Il progetto informatico «Nevo/Rialto» della polizia cantonale di Berna e della giustizia è definitivamente fallito. Il Ministero pubblico si è ritirato dal progetto a fine dicembre 2025. Da un lato, perché il ponte dati digitale pianificato originariamente tra polizia e giustizia non è stato mai realizzato. Dall'altro, perché i fornitori di Swisscom e Deloitte avevano comunicato già ad agosto 2025 che la versione SAP alla base della piattaforma non sarebbe stata più supportata a partire dal 2031.

Il progetto, avviato nel 2015/2016, era ambizioso e innovativo, ma ha avuto solo un successo parziale. Dopo un inizio zoppicante, con utenti insoddisfatti, ritardi e costi aggiuntivi, si erano poi intravisti dei progressi. Dal 2022, la polizia cantonale di Berna utilizza «Rialto» con risultati soddisfacenti e continuerà a farlo fino al 2031. Un'eventuale migrazione ad una nuova versione SAP o ad un altro sistema è attualmente oggetto di verifica. La decisione sarà presa entro metà 2026.

Il progetto, per cui inizialmente si era previsto un budget di 13,5 milioni di franchi, era finora costato, a detta del Canton Berna, circa 23 milioni di franchi. Il Cantone dovrebbe ora ricevere un importo milionario a una sola cifra a titolo di rimborso o sotto forma di prestazioni.

MOBILE WORKING

» Panasonic TOUGHBOOK con innovazioni a batteria e IA



» Gli attuali tablet e i notebook di Panasonic TOUGHBOOK

Panasonic ritiene che batterie più potenti, controllo vocale naturale, IA e connettività 5G saranno le

tendenze tecnologiche chiave per le prossime generazioni dei suoi TOUGHBOOK. Da un lato, tempi di funzionamento più lunghi e intervalli di ricarica più brevi porterebbero a una maggiore disponibilità operativa. Dall'altro, un controllo vocale migliorato consentirebbe un funzionamento affidabile e a mani libere anche in ambienti rumorosi o difficili. Le forze di intervento potrebbero così focalizzarsi sui loro compiti, mentre il dispositivo mette a disposizione le informazioni, supporta i processi o fornisce indicazioni relative al contesto con conseguenti ripercussioni positive in termini di efficienza e sicurezza sul lavoro.

Altri trend sarebbero l'IA e la connettività 5G. Grazie ad un trattamento dei dati intelligente in tempo reale, applicazioni connesse e funzioni di assistenza adattive, i robusti dispositivi terminali mobili potranno supportare ancora meglio le forze di intervento nel loro lavoro quotidiano. In parallelo, Panasonic punta a svilupparsi ulteriormente, passando da semplice fornitore di dispositivi a efficiente partner per la mobilità delle forze a girofaro blu e giallo.

Chi è interessato potrà reperire ulteriori informazioni su: <https://eu.connect.panasonic.com/it/it>

produttore

DIGITALIZZAZIONE

» CONVOTIS affina l'attenzione sulla strategia

Il CONVOTIS Group, un fornitore europeo di trasformazione digitale e soluzioni IA e su cloud, ha ceduto la sua SAP Business Unit nell'ambito di un'evoluzione strategica. In futuro, l'attenzione sarà incentrata su quattro aree tecnologiche centrali, che uniranno investimenti, attività di innovazione e capacità manageriali: trasformazione digitale e soluzioni IA per imprese e istituzioni pubbliche; soluzioni sovrane su cloud e piattaforme focalizzate sulla sovranità dei dati europei e sulla compliance; cibersicurezza, sicurezza cloud e servizi di sicurezza gestiti; modelli di servizi gestiti e su piattaforma orientati al settore.

CONVOTIS

In Svizzera, il gruppo è attivo sul mercato con la CONVOTIS Schweiz AG, con sede a Rotkreuz, nata nel 2023 dalla precedente JMC Software AG e da allora in corso di espansione. Nel 2023 ha poi acquisito la Sowatec AG (Pfäffikon ZH) e la start-up in ambito IA Innofind GmbH, nel 2024 la Berner AGENTIL e la swiss cloud computing ag (Zurigo) e nel 2025 la aspectra AG (Zurigo; ora: CONVOTIS Swiss Cloud AG). Inoltre, dal 2024 è in essere un partenariato strategico con la Diso AG (Bern), una controllata della Securize IT Solutions AG (Monaco di Baviera).

Chi è interessato potrà reperire ulteriori informazioni su: www.convotis.ch

WEF Davos:

Wenn der Blick nach oben Teil der Einsatzführung wird

Die Sicherheitsplanung am WEF in Davos findet heute dreidimensional statt – am Boden und im unteren Luftraum. Mit moderner Drohrendetektion, AI-gestützter Drohnenverifikation und abgestuften Abwehrmassnahmen wurden unerlaubte Flüge frühzeitig erkannt und abgewehrt.

Davos im Ausnahmezustand. Rund 3'000 Teilnehmende aus Politik, Wirtschaft und Wissenschaft reisen ans Weltwirtschaftsforum, darunter Staats- und Regierungsmitglieder aus aller Welt. Für die Sicherheitsorganisation bedeutet das jedes Jahr höchste Alarmbereitschaft und eine Bedrohungslage, die sich aufgrund der zunehmenden Verfügbarkeit und Verbreitung von Drohnen längst nicht mehr auf den Boden beschränkt.

«Die Sicherheitsanforderungen sind heute deutlich umfassender und komplexer. Neben den klassischen Massnahmen am Boden müssen wir zusätzliche Ebenen berücksichtigen. Dazu gehört heute selbstverständlich auch der untere Luftraum», erklärt Markus Eggenberger, Leiter Sicherheitspolizei des Polizeikorps Graubünden und verantwortlich für die sicherheitspolizeilichen Massnahmen rund um das WEF.

Flugverbotszonen müssen durchgesetzt werden

Drohnen sind frei verfügbar, technisch ausgereift und vielseitig einsetzbar. Damit steigen auch die Risiken durch unerlaubte Flüge über sensiblen Bereichen. Für das WEF gilt deshalb eine Drohnen-Flugverbotszone. Doch ein Flugverbot allein schafft noch keine Sicherheit. «Während des Anlasses besteht eine generelle Flugverbotszone, die auch für Drohnen gilt. Um diese durchzusetzen, kommt ein Drohrendetektionssystem zum Einsatz, das uns technische und personelle Interventionsmöglichkeiten bietet», erklärt Eggenberger.

Detektion, Einordnung, Intervention/Abwehr

Beim WEF 2026 setzte die Kantonspolizei Graubünden auf die Drohenschutzlösung DroneDefence von Swisscom Broadcast. Die Lösung ermöglichte den Einsatzkräften, Drohnenaktivitäten frühzeitig zu erkennen, sie korrekt einzuordnen und sie allenfalls – mit abgestuften Reaktionsmöglichkeiten – abzuwehren.

Die Lösung wurde gezielt auf die lokalen Gegebenheiten und das Schutzbedürfnis in Davos angepasst. Um die Detektionswahrscheinlichkeit zu maximieren, kamen ein Multisensor- und Multitechnologie-Ansatz zum Einsatz. Dazu gehörten auch AI-basierte Kameras, die Drohnen visuell verifizieren und eine präzisere Risikoanalyse ermöglichen. Für die Einsatzleitung bedeutet das: **Entscheidungsgrundlagen in Echtzeit.**

Abgestufte Abwehr im Einsatz

Eine der zur Verfügung gestellten abgestuften Abwehrmassnahmen war der sogenannte **Cyber Takeover**. Dabei wird die Steuerverbindung einer Drohne übernommen, um sie kontrolliert aus dem Schutzbereich zu führen oder an einem definierten Ort landen zu lassen. Während des WEF wurden Drohnen innerhalb der Flugverbotszone detektiert. Entscheidend war dabei weniger die Anzahl als die Reaktionsfähigkeit: Die Einsatzleitung konnte die Vorfälle frühzeitig erkennen, rasch einordnen und entsprechende Massnahmen einleiten.



DroneDefence von Swisscom Broadcast wächst modular je nach Schutzbedarf: Von punktueller Detektion bis zur multisensorischen Lösung mit Kamera, Radar und Abwehrmöglichkeiten.

Die Lösung ist überall schnell einsatzbereit, da Swisscom Sendemasten zur Installation dienen.



WEF Davos:

Quand la surveillance aérienne s'intègre pleinement à la conduite des interventions

Au WEF de Davos, la planification de la sécurité se conçoit aujourd'hui en trois dimensions – au sol et dans l'espace aérien inférieur. Grâce à une détection moderne des drones, à une vérification par drones basée sur l'IA et à des mesures de défense échelonnées, les vols non autorisés ont été détectés à un stade précoce et neutralisés.

Davos en état d'urgence. Près de 3000 participant-e-s issus des milieux politique, économique et scientifique, parmi lesquels des chefs d'État et de gouvernement du monde entier, assistent au Forum économique mondial. Pour l'organisation de la sécurité, cela implique chaque année un état d'alerte maximal et une situation de menace qui, compte tenu de la disponibilité et de la diffusion croissantes des drones, ne se limite plus au sol.

«Les exigences en matière de sécurité sont aujourd'hui beaucoup plus étendues et complexes. Outre les mesures classiques au sol, nous devons prendre en compte d'autres niveaux. L'espace aérien inférieur en fait bien entendu partie», explique Markus Eggenberger, responsable de la police de sécurité du corps de police des Grisons et responsable des mesures de sécurité policière déployées dans le cadre du WEF.

Les zones d'exclusion aérienne doivent être respectées

Les drones sont librement accessibles, techniquement au point et polyvalents, ce qui renforce les risques liés aux vols non autorisés au-dessus de zones sensibles. Une zone d'exclusion des drones s'applique par conséquent pour le WEF. Une interdiction de vol ne suffit toutefois pas à elle seule à créer un contexte sécurisé. «Une zone d'exclusion aérienne générale, également valable pour les drones, s'applique pendant l'événement. Nous utilisons un sys-

tème de détection de drones qui nous offre des possibilités d'intervention techniques et humaines», explique M. Eggenberger.

Détection, classification, intervention/défense

Lors du WEF 2026, la police cantonale des Grisons a fait le choix de la solution de protection contre les drones DroneDefence de Swisscom Broadcast. Cette solution a permis aux forces d'intervention d'identifier à un stade précoce les activités de drones, de les classer correctement et, le cas échéant, de les repousser en appliquant des mesures de réaction échelonnées.

La solution a été spécifiquement adaptée aux conditions locales et au besoin de protection à Davos. Afin de maximiser la probabilité de détection, une approche combinant plusieurs capteurs et plusieurs technologies a été utilisée. Celle-ci intégrait également des caméras basées sur l'IA qui vérifient visuellement les drones et permettent une analyse plus précise des risques. Le chef d'intervention a ainsi disposé de **bases décisionnelles en temps réel**.

Une défense échelonnée en action

L'une des mesures de défense échelonnées mises à disposition était ce que l'on appelle le Cyber Takeover. Cette

technique consiste à prendre le contrôle de la liaison de commande d'un drone afin de le guider de manière contrôlée hors de la zone protégée ou de le faire atterrir à un endroit défini. Pendant le WEF, drones ont été détectés à l'intérieur de la zone d'exclusion aérienne. Ce n'est pas tant le nombre que la réactivité qui a joué un rôle décisif: la direction des interventions a pu identifier les incidents à un stade précoce, les classer rapidement et prendre les mesures requises.

DroneDefence de Swisscom Broadcast évolue de manière modulaire en fonction des besoins de protection: de la détection ponctuelle à la solution multisensorielle intégrant caméra, radar et moyens de défense. La solution est rapidement opérationnelle n'importe où, les antennes émettrices de Swisscom étant utilisées pour l'installation.



Miele

Ihr schützt Leben. Wir schützen eure Ausrüstung.



Wir verstehen, welchen Herausforderungen und Gefahren Feuerwehren und andere Einsatzkräfte täglich gegenüberstehen.

Um die zu schützen, die andere schützen, bieten wir 360PRO.

Entdecken Sie mehr unter: www.miele.ch/pro/feuerwehr

Miele Professional. Immer Besser.

360 PRO



Eine Plattform für den landesweiten Informationsaustausch im Rettungswesen

Eilen Rettungskräfte zu einem Einsatz, handelt es sich meist um ein «kooperatives Ereignis», in dem Fachleute diverser Organisationen Hand in Hand agieren – häufig aus unterschiedlichen Regionen oder sogar Kantonen. Damit dabei alle jederzeit über sämtliche relevanten Informationen verfügen, hat die sureVIVE AG gemeinsam mit Partnern nun das Projekt «Swiss Emergency Data Hub» (SEDH) lanciert.



» Bei einer Vielzahl von Ereignissen – hier bei einem Verkehrsunfall – stehen Mitglieder verschiedener Rettungsorganisationen kooperativ im Einsatz. Künftig soll die Zusammenarbeit noch besser werden, basierend auf einem einheitlichen Echtzeit-Lagebild. Dazu wurde das Projekt «SEDH» initiiert, das derzeit von der sureVIVE AG mit mehreren Partnern und Pilotkantonen umgesetzt wird.

Passiert in der Schweiz ein Unglück, sind die Einsatzkräfte der Sicherheits- und Rettungsorganisationen jederzeit zur Stelle, um zu helfen, zu retten, zu bergen oder zu löschen. Dabei erfordert in der Regel jedes Ereignis – vom Schmelbrand in der Küche bis zum überregionalen Grossereignis wie einer kantonsübergreifenden Naturkatastrophe – das Zusammenwirken von Kräften unterschiedlicher Organisationen. Beispielsweise Feuerwehr, Sanität und Polizei – oder auch Strassen-, Luft-, Berg-, Höhen-, Tiefen- und Gewässerretter sowie First Responder (FR), Geländesuchhunde, Zivil- und Katastrophenschutz.

Jede Organisation der Schweizer Blaulichtfamilie dient spezifischen Zwecken, hat individuelle Stärken, verfügt über spezialisierte Fachpersonen und die dazu passenden Einsatzmittel. Im Verbund der Kräfte entsteht ein leistungsstarkes Miteinander, aus dem heraus die ereignisspezifisch geforderten Leistungen erbracht werden – schnell, effizient, mit hoher Qualität und Sicherheit.



» Ein Lawinenunglück wie jenes am 26. Dezember 2019 in Andermatt ist ein gutes Beispiel für einen kooperativen Einsatz. Damals standen 40 ARS-Bergretter, die Rega, der kommerzielle Helikopterbetreiber Swiss Helicopter AG, 20 zivile Helfer, 5 Suchhundeteams, die Kantonspolizei Uri sowie Angehörige der Bergbahnen und der Sanität im Einsatz.

Beispiel: Lawinenunglück im Wintersportgebiet

Ein gutes Beispiel liefert ein (fiktives) Lawinenunglück im Skigebiet. Gleichgültig, wer dieses meldet – eine Privatperson, ein Disponent der Bergbahn oder ein Pistenpatrouilleur: Der Alarm, der bei der Einsatzzentrale der Rega über deren Alarmnummer 1414 angenommen wird, setzt eine Kaskade in Gang. Diese bindet Einsatzkräfte unterschiedlicher Organisationen ein: Pistenrettungsdienste, Fachspezialisten, Lawinenhundeführer und Rettungsstationen der Alpinen Rettung Schweiz (ARS), Polizei, Sanität und die Rega selbst. Hinzu kommen bisweilen zivile Institutionen – etwa kommerzielle Helikopterfirmen, die Transporteinsätze leisten – oder, in gewissen Fällen, First Responder oder Peers.

Kooperation und Kommunikation sind das A und O für den Erfolg

Damit das interorganisatorische und nicht selten auch überregionale Miteinander optimal gesteuert und koordiniert werden kann, ist für den gemeinsamen Erfolg ein Faktor eminent: ein gemeinsames Lagebild, basierend auf in Echtzeit verteilten Informationen und Daten, sowie eine jederzeit allen zugängliche Kommunikationslösung.

Im genannten Beispiel eines Lawinenunglücks, bei dem eine hohe Geschwindigkeit der Hilfe einen kritischen Faktor darstellt, müssen Manpower und Materialien schnell und gezielt zum Einsatz kommen. Mithilfe eines einheitlichen Lagebilds

können beispielsweise Helikopter effizient Einsatzkräfte aufnehmen, Anflugzeiten abgeschätzt und die Lage am Lawinenkegel überblickt werden. Zudem wirkt sich die Sichtbarkeit von Helikoptern im gemeinsamen Lagebild positiv auf die Flugsicherheit aus.

Dabei ist die erste Phase im Einsatz ebenso entscheidend für die erfolgreiche Gesamtbewältigung des Ereignisses wie alle nachfolgenden Schritte, die mit einem «Aufwachsen» der Kräfte und Mittel einhergehen. Entsprechend müssen Menschen, Fahrzeuge und Helikopter lageabhängig ins System eingebunden werden können – jederzeit, einfach manuell oder automatisiert, hochverfügbar und Hardware-unabhängig.

Live-Lagebild und Einsatzleitung dank Lösungen von sureVIVE

Eine bewährte Lösung für das skizzierte Beispiel besteht seit 2021 mit «Alpine Rescue Mission Control» (ARMC). Diese basiert auf dem SaaS-Tool «Momentum PRO» und dient der Alarmierung, Einsatzführung und Lagebilddarstellung bei terrestrischen und luftgestützten Rettungseinsätzen (siehe auch BLAULICHT 04-2024). Entwickelt wurde das System von der sureVIVE AG mit Sitz in Mendrisio, die es auch betreibt. «Im Fall einer Notsituation im Berggebiet, für welche die ARS den Einsatz übernehmen soll, werden deren Rettungskräfte sowie allfällig benötigte weitere Rettungskräfte, etwa Pistenretter, via «ARMC» aufgeboden. Die Alarmierung erfolgt über die Sanitätsnotrufnummer 144 oder die Alarmnummer 1414 der Rega, die in solchen Fällen meist auch die Einsatzkoordination übernimmt», erklärt sureVIVE-CEO Georg Hauzenberger.

Das Aufgebot der Kräfte nach der Alarmierung kann so dann – dank eines flexiblen, intelligenten Algorithmus – vollautomatisch nach dem «Next-Best»-Prinzip erfolgen. Oder, bei Bedarf, auch manuell selektiv.

Unmittelbar nach der Alarmierungs- und Aufgebotphase mutiert die Lösung nahtlos zum Einsatzleit- und Lagebildsystem, mit dessen Hilfe die disponierten Einsatzkräfte überwacht, informiert und geleitet werden. «Dabei können auch weitere, während der Aufwuchs-



» Mit «MOMENTUM PRO», «ARMC» und Threema-Gruppenchats verfügt sureVIVE über ein von bereits 22 Kantonen und zahlreichen Rettungsorganisationen genutztes System für Alarmierung, Einsatzleitung, Echtzeit-Lagebild und Einsatzkommunikation. Dieses ist als Web-Applikation und als mobile App verfügbar – und wird nun, ergänzt um weitere Komponenten, zum SEDH weiterentwickelt.

phase hinzustossende Kräfte eingebunden werden», erläutert Georg Hauzenberger. «Während des gesamten Einsatzes haben alle dank des kartenbasierten Live-Lagebilds zu jedem Zeitpunkt den perfekten Überblick.»

Überdies können – im Sinn eines Ökosystems der besten IT-Systeme – aus «Momentum PRO» und damit auch aus «ARMC» heraus automatisch Gruppen in der sicheren und datenschutzkonformen Kommunikationsapp Threema erstellt werden, die von allen beteiligten Einsatzkräften zur multimedialen Kommunikation genutzt werden können (siehe auch BLAULICHT 04-2025).

Rega will das bewährte System mit Partnern zum SEDH emanzipieren

Die Rega war vom Start weg massgeblich in die Entwicklung involviert. Sie nutzt das System in ihrer Einsatzleitzentrale, um Notfalleinsätze der ARS-Bergretter und deren First-Responder-Plus-Gruppen (FR+) sowie weiterer Rettungskräfte, etwa der Gewässerretter in der Ostschweiz, auszulösen, zu koordinieren, zu unterstützen und zu leiten. Auch bei Pistenrettungsdiensten wird das System schweizweit immer mehr eingesetzt – mit dem Ziel, diese effizienter in die Rettungskette einzubinden und sogar die elektronische Anforderung von Rettungshelikoptern und potenziell Ambulanzen zu ermöglichen.

Nach nunmehr fast fünf Jahren erfolgreicher Arbeit mit dem System in nahezu der ganzen Schweiz will die Rega es gemeinsam mit Blaulicht- und Industriepartnern skalieren – und zum «Swiss Emergency Data Hub» weiterentwickeln. Dieser soll allen interessierten Organisationen der Schweizer Blaulichtfamilie zur Anbindung offenstehen, damit diese Einsatzinformationen miteinander teilen können. «Eigenbestimmt und rollenbasiert, anhand strenger Kriterien bezüglich Datenhoheit und Datenschutz», wie Georg Hauzenberger betont.

Diese Intention steht hinter dem Projekt SEDH

Die Idee des SEDH ist so bestechend einfach wie logisch. Als national engagierte Luftrettungsorganisation agiert die Rega seit jeher regionenübergreifend. Zudem ist sie immer interorganisatorisch tätig – im Verbund mit den am jeweiligen Einsatzort zuständigen Kräften. Entsprechend eminent ist ihr Bedarf für einen effizienten und sicheren Informations- und Datenaustausch über institutionelle sowie regionale respektive kantonale Grenzen hinweg.

Bislang sieht sich die schweizweit tätige Rega dabei mit zwei wesentlichen Hemmschwellen konfrontiert: Mit der oftmals technisch bedingten «Blindheit» lokal verankerter Organisationen für alles, was ausserhalb der eigenen, räumlich wie organisatorisch nicht selten eng gesteckten Grenzen geschieht. Und mit der Tatsache, dass es in der Schweiz bislang weder eine nationale Sanitätsnotrufzentrale (SNZ) noch ein landesweites digitales Ökosystem gibt, das im Fall eines Ereignisses Live-Informationen zu personellen Ressourcen sowie verfügbaren Einsatzmitteln liefern könnte – für alle und von allen in ein bestimmtes Ereignis eingebundenen Kräfte.



» Georg Hauzenberger, CEO von sureVIVE: «Grenzen, aufgrund derer Einsatzkräfte kooperierender Rettungsorganisationen nicht dasselbe Lagebild haben, müssen eingerissen werden. Das Projekt SEDH führt zur 'Demokratisierung des Rettungswesens' – zum Vorteil aller, die darin mitwirken.»

Beide Faktoren wirken sich negativ auf die Möglichkeit aus, ein gemeinsames Lagebild aller in ein Ereignis involvierten Einsatzkräfte zu nutzen und jederzeit stringent das Prinzip «Next best» anwenden zu können. Aufgrund der Kleinteiligkeit der Schweiz und ihrer föderalistischen Strukturen besteht ein historisch gewachsener Flickenteppich aus Zuständigkeiten, Organisationen und Einsatzräumen. Entsprechend mühsam gestaltet sich nicht selten der Austausch einsatzrelevanter Informationen bei kooperativen Einsätzen. Informationsinseln sind die Regel – und Brüche in der Informations- oder Datenweiterleitung fast schon der Normalfall. Nun soll sich das ändern – mit dem «Swiss Emergency Data Hub».

Essenzielle Informationen teilen – selbstbestimmt und sicher

Dieser befindet sich bereits in der Entwicklung und soll im Ereignisfall alle relevanten Informationen an einem Ort bündeln – mit Zugriff für alle involvierten Organisationen. Eine grosse Herausforderung dabei waren die strengen Datenschutzrichtlinien sowie die unantastbare Dispositions- und Datenhoheit jeder Organisation. «Beidem trägt der SEDH umfassend Rechnung», betont daher Programmleiter Martin Thalmann. «Auf dem Hub werden Daten gestreamt – aber nicht gespeichert. Zudem entscheidet jede angebundene Organisation selbstbestimmt, mit wem sie Daten teilen will – und welche Daten sie teilen will.» Überdies werden die Daten wie bei «Momentum PRO» rollenbasiert gestreamt. «Beispielsweise ist es nicht möglich, dass eine Sanitätsorganisation sensible Patientendaten mit einem privaten Helikopterunternehmen, das Transportflüge leistet, teilt respektive dass Letzteres wie auch immer Zugriff auf solch sensible Daten erlangen könnte», versichert Martin Thalmann.

Nutzung bestehender Technologien

So visionär das Projekt SEDH klingt: Die digitale Welt muss dafür nicht neu erfunden werden. Denn mit «Momentum PRO», «ARMC» sowie der von sureVIVE und Threema für die ARS realisierten «Dynamischen Gruppenkommunikation» über Threema Work existieren wesentliche, in der Praxis bewährte Bausteine bereits. Ergänzt werden sie um Lösungen zur Verteilung von Informationen. «Auch die gibt es schon. Wir wenden sie für den SEDH lediglich in einem neuen Kontext an – und mit bisher nicht gekannter Rigorosität», verrät Georg Hauzenberger.

Komplett neu gedacht werden musste indes die Architektur der Schnittstellen, wie er erläutert: «Klassische Punkt-zu-Punkt-Verbindungen hätten eine sehr hohe Anzahl von Schnittstellen bedingt, was die Betriebskomplexität und die Kosten für Blaulichtorganisationen treibt. Das kam nicht infrage. Stattdessen setzen wir auf eine ereignisgesteuerte Architektur. Alles findet auf dem SEDH statt – und jede Organisation benötigt daher nur eine einzige Schnittstelle: die zum Hub.»

Diese Schnittstellen werden derzeit von renommierten Schweizer Spezialanbietern wie beispielsweise Hexagon, LogObject, Swisscom und sureVIVE entwickelt. Das Ziel: Interessierte Organisationen sollen sich über standardisierte Verbindungen auf dem «SEDH» einloggen können – unabhängig von und passgenau zu ihren jeweiligen ELZ-Lösungen. «Bei der Konfiguration der Schnittstelle zum Hub kann dann exakt definiert werden, welche Informationen mit welchen anderen Organisationen geteilt werden sollen – und welche nicht», erklärt Georg Hauzenberger.

Nur eine einzige Schnittstelle ist nötig – zum SEDH

Im Ereignisfall werden ereignisrelevante Informationen also niemals auf dem SEDH gespeichert, sondern über diesen gestreamt und entsprechend den jeweiligen Konfigurationen der Schnittstellen geteilt. So werden Informationen, die von einer Organisation produziert werden (beispielsweise von einer kantonalen SNZ, welche aufgrund einer Alarmmeldung einen Einsatz auslöst), den anderen in das Ereignis eingebundenen Akteuren zugänglich gemacht. Letztere nehmen sie auf, stellen sie dar, verarbeiten sie weiter – etwa, indem die SNZ einen Rettungswagen entsendet, die Rega einen Helikopter und die jeweilige kantonale FR-Organisation oder die ARS einen First Responder oder First Responder+. Diese Informationen fließen zurück – und über den Hub zu den anderen Partnern. Alle involvierten Einsatzleitstellen und im Einsatz befindlichen Rettungskräfte wissen sofort: Der Rettungswagen, die Rega und die First Responder sind unterwegs. Und natürlich sehen sie auf der Live-Karte auch, wo sich diese aktuell befinden.

«So entsteht ein detailliertes dynamisches Live-Lagebild. Alle wissen, was bereits veranlasst und getan wurde, was aktuell läuft, wer sich wo befindet – und was die nächsten Schritte sein müssen», erklärt Adrian Schindler, Mediensprecher der Rega. «Ressourcen, Handlungen und Einsatzmittel werden für alle transparent. Das erleichtert und intensiviert das Teamwork, ermöglicht faktenbasierte

Entscheide in kürzerer Zeit, vermeidet Nachfragen, Missverständnisse und Fehlinterpretationen. Kooperative Einsätze können dadurch schneller, effizienter und sicherer bewältigt werden.»

Mit dieser grundlegenden Zielsetzung steht das Projekt übrigens dediziert im Einklang mit dem vom Interverband Rettungswesen (IVR) in dessen «Vision Rettungswesen Schweiz 2034» formulierten Ziel der durchgängigen Digitalisierung der Schweizer Rettungskette.

Entwicklung im kooperativen Verbund

Ganz nach dem Vorbild der Einsatzkräfte am Schadenplatz, wirken auch im Projekt SEDH zahlreiche Partner unterschiedlicher Institutionen mit. Die Rega ist Auftraggeberin und stemmt die Anschubfinanzierung. Die sureVIVE AG agiert als Entwicklerin, Lieferantin und Plattformbetreiberin der ersten Stunde. Vonseiten der Industrie sind im Teilprojekt «Architektur» namhafte Anbieter aus den Bereichen Einsatzleitung, Alarmierungslösungen und Einsatzkommunikation mit an Bord. Und im Teilprojekt «Nutzer» engagieren sich neben der Rega mit der ARS und weiteren Partnern auch drei Pilotkantone: der Kanton Graubünden, der einst als erster Kanton die ARS mit dem Aufbau eines FR+-Dispositivs beauftragte und entsprechend langjährige Erfahrung mit den ARS-Apps hat. Der Kanton St. Gallen, der im Bereich der Wasserrettung, wo die Polizeitaucher der Kantonspolizei St. Gallen, die Kräfte der SLRG Mittelrheintal und die Fachspezialisten Canyoning der Alpinen Rettung Ostschweiz (ARO) kooperieren, viel Erfahrung mit Kooperationen über Institutions- und Kantonsgrenzen hinweg mitbringt. Und der Kanton Tessin, der bei den schweren Unwetterereignissen 2024 im Misox, im Maggialtal und im Val Bavona viel Leid erfuhr – aber auch umfassende Praxiserfahrungen zur kantons- und organisationsübergreifenden Kooperation der Rettungskräfte sammeln konnte, die nun in wertvolle Beiträge für den SEDH münden werden.

Mitarbeit im Teilprojekt «Nutzer» ist möglich

Wie beim Aufwuchs der Kräfte im Ereignisfall wird die Zahl der im Projekt SEDH engagierten Personen, Firmen und Organisationen sowie Kantone noch wachsen – was durchaus geplant ist, wie Martin Thalmann erläutert: «Interessierte, die am SEDH-Projekt mitarbeiten wollen, insbesondere in der Gruppe <Nutzer>, sind eingeladen, Kontakt zu uns aufzunehmen.» Schliesslich zielt das Projekt auf eine breite Basis zugunsten landesweiter Akzeptanz und Nutzung. Daher ist laut Martin Thalmann auch angedacht, dass der SEDH ab einem bestimmten Stadium von einer noch zu formierenden Trägerschaft verwaltet, finanziert und weiterentwickelt wird. Von und zum Nutzen der beteiligten Organisationen – und für die Menschen, die in der Schweiz in eine Notlage geraten, welche im kooperativen Verbund bewältigt werden muss.

Mehr Infos erhalten interessierte Organisationen über die Firma sureVIVE AG auf der Website www.sedh.ch, per E-Mail an connect@sedh.ch oder telefonisch unter der Nummer 091 646 29 04.

Une plateforme pour l'échange d'informations à l'échelle nationale dans le domaine des services de secours

Lorsque les forces de secours interviennent, il s'agit généralement d'un « événement coopératif » dans lequel des experts de diverses organisations travaillent main dans la main, souvent issus de différentes régions, voire de différents cantons. Afin que chacun dispose à tout moment de toutes les informations pertinentes, l'entreprise sureVIVE AG a lancé, en collaboration avec des partenaires, le projet « Swiss Emergency Data Hub » (SEDH).



» Lors de nombreux événements, comme ici lors d'une intervention suite à une avalanche dans les Alpes suisses, les membres de différentes organisations de sauvetage coopèrent. À l'avenir, la collaboration devrait encore s'améliorer grâce à une image uniforme de la situation en temps réel. Le projet « SEDH » a été lancé à cette fin et est actuellement mis en œuvre par l'entreprise sureVIVE AG.

En cas d'accident en Suisse, les forces d'intervention des organisations de sécurité et de sauvetage sont toujours présentes pour apporter leur aide, secourir, évacuer ou éteindre des incendies. En règle générale, chaque événement (du feu couvant dans une cuisine à un événement majeur suprarégional tel qu'une catastrophe naturelle touchant plusieurs cantons) nécessite la collaboration des forces de différentes organisations. Par exemple, les pompiers, les services médicaux et la police, mais également les sauveteurs routiers, aériens, en montagne, en hauteur, en profondeur et aquatiques, ainsi que les First Responder

(FR - premiers intervenants), les chiens de recherche en terrain accidenté, la protection civile et la protection contre les catastrophes.

Chaque organisation de la famille suisse des services d'urgence poursuit des objectifs spécifiques, possède des atouts individuels, dispose de spécialistes et des moyens d'intervention adaptés. La mise en commun des forces crée une synergie performante qui permet de fournir les prestations requises en fonction de l'événement, de manière rapide, efficace, avec un niveau élevé de qualité et de sécurité.



» La Rega est active dans toute la Suisse et coopère en permanence avec les forces locales d'autres organisations (de sauvetage), comme ici lors d'un exercice avec la police, les pompiers et les services médicaux. À l'avenir, celles-ci devraient pouvoir partager des informations en temps réel via le SEDH, dans le respect de la protection des données et de manière autonome.

Exemple : Avalanche dans une station de sports d'hiver

L'avalanche (fictive) dans une station de ski est un bon exemple. Peu importe qui la signale : un particulier, un responsable des remontées mécaniques ou un pisteur-secouriste : l'alerte, qui est reçue par la centrale d'intervention de la Rega via son numéro d'urgence 1414, déclenche une cascade d'événements. Elle mobilise les forces d'intervention de différentes organisations : services de secours sur les pistes, spécialistes, maîtres-chiens d'avalanche et stations de secours du Secours Alpin Suisse (SAS), police, services médicaux et la Rega elle-même. À cela s'ajoutent parfois des institutions civiles, telles que des sociétés d'hélicoptères commerciales qui assurent des missions de transport ou, dans certains cas, des First Responder ou des peers.

La coopération et la communication sont essentielles pour garantir le succès de l'intervention

Afin de garantir une gestion et une coordination optimales de la coopération interorganisationnelle et souvent supra-régionale, un facteur est essentiel pour la réussite commune : une image commune de la situation, fondée sur des informations et des données distribuées en temps réel, ainsi qu'une solution de communication accessible à tous à tout moment.

Dans l'exemple cité d'une avalanche, où la rapidité des secours est un facteur critique, les ressources humaines et matérielles doivent être mobilisées rapidement et de manière ciblée. Grâce à une image uniforme de la situation, les hélicoptères peuvent, par exemple, embarquer efficacement les forces d'intervention, estimer les temps d'approche et avoir une vue d'ensemble de la situation au niveau de la coulée de neige. De plus, la visibilité des hélicoptères dans l'image commune de la situation a un effet positif sur la sécurité des vols.

La première phase de l'intervention est tout aussi décisive pour la réussite globale de la gestion de l'événement que toutes les étapes suivantes, qui s'accompagnent d'une « augmentation » des forces et des moyens. Par conséquent, les personnes, les véhicules et les hélicoptères doivent pouvoir être intégrés dans le système en fonction de la situation, à tout moment, de manière simple, manuelle ou automatisée, avec une haute disponibilité et indépendamment du matériel.

Image en temps réel de la situation et gestion des interventions grâce aux solutions de sureVIVE

Une solution éprouvée pour l'exemple décrit existe depuis 2021 avec « Alpine Rescue Mission Control » (ARMC). Elle repose sur l'outil SaaS « Momentum PRO » et sert à l'alerte, à la gestion des interventions et à la représentation de la situation lors d'opérations de sauvetage terrestres et aériennes (voir également BLAULICHT 04-2024). C'est l'entreprise sureVIVE AG, basée à Mendrisio, qui a développé le système et qui l'exploite. « En cas d'urgence en montagne, pour laquelle le SAS doit intervenir, ses secouristes ainsi que tout autre secouriste éventuellement nécessaire, tel que des pisteurs-secouristes, sont mobilisés via < ARMC >. L'alerte est donnée via le numéro d'urgence médicale 144 ou le numéro d'urgence 1414 de la Rega, qui prend généralement en charge la coordination des interventions dans de tels cas », explique Georg Hauzenberger, PDG de sureVIVE.

Grâce à un algorithme flexible et intelligent, la mobilisation des forces après l'alerte peut alors se faire de manière entièrement automatique selon le principe du « next-best » (c'est toujours l'unité disponible la plus rapide et la mieux adaptée qui est alertée). Ou, si nécessaire, de manière manuelle et sélective.

Immédiatement après la phase d'alerte et de mobilisation, la solution se transforme en un système de gestion des interventions et de représentation de la situation, qui permet de surveiller, d'informer et de diriger toutes les forces réparties. « D'autres forces qui arrivent pendant la phase de mobilisation intense peuvent également être intégrées », explique Georg Hauzenberger. « Grâce à l'image en temps réel de la situation, chacun dispose à tout moment d'une vue d'ensemble parfaite pendant toute la durée de l'intervention. »



» Les applications « MOMENTUM PRO », « ARMC » et la communication de groupe dynamique via Threema ont fait leurs preuves dans le cadre de la coopération entre la Rega, le SAS, les forces du CAS et les First Responder. Le système est désormais en cours de développement pour devenir le SEDH, utilisable à l'échelle nationale.

De plus, dans l'esprit d'un écosystème regroupant les meilleurs systèmes informatiques, « Momentum PRO » et donc « ARMC » permettent de créer automatiquement des groupes dans l'application de communication sécurisée et conforme à la protection des données Threema, qui peuvent être utilisés par toutes les forces d'intervention impliquées pour la communication multimédia (voir également GYROPHARE BLEU 04-2025).

La Rega souhaite émanciper ce système éprouvé avec ses partenaires pour en faire le SEDH

La Rega a été impliquée de manière significative dans le développement du système dès le début. Elle utilise ce dernier dans sa centrale d'intervention pour déclencher, coordonner, soutenir et diriger les interventions d'urgence des sauveteurs en montagne du SAS et de leurs groupes First Responder Plus (FR+), ainsi que d'autres équipes de secours, telles que les sauveteurs aquatiques en Suisse orientale. Le système est également de plus en plus utilisé par les services de secours sur pistes dans toute la Suisse, dans le but de les intégrer plus efficacement dans la chaîne de sauvetage et même de permettre la demande électronique d'hélicoptères de sauvetage et éventuellement d'ambulances.

Après près de cinq ans d'utilisation fructueuse du système dans presque toute la Suisse, la Rega souhaite, en collaboration avec ses partenaires des organisations d'urgence et de l'industrie, le développer pour en faire le « Swiss Emergency Data Hub ». Celui-ci sera accessible à toutes les organisations intéressées des services d'urgence suisses afin qu'elles puissent partager entre elles les informations relatives aux interventions. « De manière autonome et en fonction des rôles, selon des critères stricts en matière de souveraineté et de protection des données », comme le souligne Georg Hauzenberger.

Voici l'intention qui sous-tend le projet SEDH

L'idée du SEDH est aussi simple que logique. En tant qu'organisation nationale de sauvetage aérien, la Rega a toujours opéré au-delà des frontières régionales. Elle travaille en outre toujours de manière interorganisationnelle, en collaboration avec les forces compétentes sur le lieu d'intervention. Il est donc essentiel pour elle de pouvoir échanger des informations et des données de manière efficace et sécurisée au-delà des frontières institutionnelles, régionales et cantonales.

Jusqu'à présent, la Rega, active dans toute la Suisse, est confrontée à deux obstacles majeurs : d'une part, la « cécité » souvent technique des organisations locales pour tout ce qui se passe en dehors de leurs propres frontières, souvent étroites tant sur le plan géographique qu'organisationnel. D'autre part, il n'existe à ce jour en Suisse ni centrale nationale d'appel d'urgence sanitaire (SNZ) ni écosystème numérique national capable de fournir en temps réel, en cas d'incident, des informations sur les ressources humaines et les moyens d'intervention disponibles, pour toutes les forces impliquées dans un incident donné et provenant de toutes ces forces.

» Georg Hauzenberger, PDG de sureVIVE : « Tous les composants fondamentaux du projet SEDH sont déjà en place. Nous mettons actuellement en place les interfaces, chaque organisation n'ayant besoin que d'une seule : celle menant vers la plateforme. »

Ces deux facteurs ont un impact négatif sur la possibilité d'utiliser une image commune de la situation de toutes les forces d'intervention impliquées dans un événement et d'appliquer à tout moment le principe du « next-best ». En raison de la fragmentation de la Suisse et de ses structures fédéralistes, il existe un ensemble disparate de compétences, d'organisations et de zones d'intervention qui s'est constitué au fil de l'histoire du pays. Il n'est donc pas rare que l'échange d'informations pertinentes pour les interventions coopératives s'avère laborieux. Les îlots d'information sont la règle, et les ruptures dans la transmission des informations ou des données sont presque la norme. Cela devrait désormais changer grâce au « Swiss Emergency Data Hub ».



Partager des informations essentielles, de manière autonome et sécurisée

Ce système est déjà en cours de développement et, en cas d'événement, il permettra de regrouper toutes les informations pertinentes en un seul endroit, accessible à toutes les organisations impliquées. Les directives strictes en matière de protection des données ainsi que la souveraineté inviolable de chaque organisation en matière de coordination et de données ont constitué un défi majeur. « Le SEDH tient pleinement compte de ces deux aspects », souligne Martin Thalmann, responsable du programme. « Les données sont diffusées sur la plateforme, mais ne sont pas stockées. De plus, chaque organisation connectée décide de manière autonome avec qui elle souhaite partager ses données et quelles données elle souhaite partager. » Et comme dans « Momentum PRO », les données sont diffusées en fonction des rôles. « Par exemple, il n'est pas possible qu'une organisation médicale partage des données sensibles sur des patients avec une entreprise privée d'hélicoptères qui effectue des vols de transport, ni que cette dernière puisse avoir accès à de telles données sensibles », assure Martin Thalmann.

Utilisation des technologies existantes

Même si le projet SEDH paraît visionnaire : il n'est pas nécessaire de réinventer le monde numérique pour le mettre en œuvre. En effet, avec « Momentum PRO », « ARMC » et la « communication de groupe dynamique » via Threema Work, mise en œuvre par sureVIVE et Threema pour le SAS, il existe déjà des éléments essentiels qui ont fait leurs preuves dans la pratique. Ces éléments sont complétés par des solutions de diffusion d'informations. « Celles-ci existent également déjà. Nous les utilisons simplement dans un nouveau contexte pour le SEDH, et avec une rigueur sans précédent », révèle Georg Hauzenberger.

Swiss Business Quality  since 1996

Kommando/ Einsatzleitfahrzeuge für Polizei, Rettungsdienst, Feuerwehr...



Sofort verfügbare Einsatzfahrzeuge



2021 Landrover Defender 110 SD6
Automatikgetriebe, 13'000 km,
Luftfederung / LED Warnanlage



2024 Ford Ranger Wildtrak 3.0 V6
Automatikgetriebe, 9'500 km,
Anhängerkupplung



2012 Volvo XC70 T6 AWD
Automatikgetriebe, 27'000 km,
Heckausbau mit Schubladen



ACT
special car center
güterstrasse 21
ch-5014 gretzenbach / so

telefon
+41 (0)62 724 09 59
telefax
+41 (0)62 724 09 58
info@act-specialcar.ch
www.act-specialcar.ch

Das alles und noch viel mehr finden Sie bei uns

L'architecture des interfaces a toutefois dû être entièrement repensée, comme il l'explique : « Les connexions point à point classiques auraient nécessité un nombre très élevé d'interfaces, ce qui aurait augmenté la complexité opérationnelle et les coûts pour les organisations d'urgence. Cela n'était pas envisageable. Nous avons donc opté pour une architecture événementielle. Tout se passe sur le « SEDH », et chaque organisation n'a donc besoin que d'une seule interface : celle menant à la plateforme. »

Ces interfaces sont actuellement développées par des fournisseurs spécialisés suisses renommés tels que Hexagon, LogObject, Swisscom et sureVIVE. L'objectif : Les organisations intéressées doivent pouvoir se connecter au SEDH via des connexions standardisées, indépendamment de leurs solutions ELZ (de centrale d'intervention) respectives et en parfaite adéquation avec celles-ci. « Lors de la configuration de l'interface vers la plateforme, il est alors possible de définir précisément quelles informations doivent être partagées avec quelles autres organisations, et lesquelles ne doivent pas l'être », explique Georg Hauzenberger.

Une seule interface est nécessaire, celle menant vers le SEDH

En cas d'événement, les informations pertinentes ne sont donc jamais stockées sur le SEDH, mais diffusées en continu via celui-ci et partagées conformément aux configurations respectives des interfaces. Ainsi, les informations produites par une organisation (par exemple par une SNZ [centrale d'appel d'urgence sanitaire] cantonale qui déclenche une intervention à la suite d'une alerte) sont mises à la disposition des autres acteurs impliqués dans l'événement. Ces derniers les enregistrent, les affichent et les traitent, par exemple en envoyant une ambulance depuis la SNZ, un hélicoptère depuis la Rega et un First Responder ou First Responder+ depuis l'organisation FR cantonale du SAS. Ces informations sont transmises aux autres partenaires via la plateforme. Toutes les centrales d'intervention impliquées et les équipes de secours en intervention sont immédiatement informées : l'ambulance, la Rega et les First Responder sont en route. Et bien sûr, elles peuvent également voir sur la carte en temps réel où elles se trouvent actuellement.

« Cela permet d'obtenir une image détaillée et dynamique de la situation en temps réel. Tout le monde sait ce qui a déjà été mis en place et fait, ce qui est en cours, qui se trouve où et quelles doivent être les prochaines étapes », explique Adrian Schindler, porte-parole de la Rega. « Les ressources, les actions et les moyens d'intervention deviennent transparents pour tous. Cela facilite et intensifie le travail d'équipe, permet de prendre des décisions fondées sur des faits en moins de temps, évite les demandes de précisions, les malentendus et les interprétations erronées. Les interventions coopératives peuvent ainsi être menées plus rapidement, plus efficacement et de manière plus sûre. »

Avec cet objectif fondamental, le projet s'inscrit par ailleurs en parfaite cohérence avec l'objectif de numérisation complète de la chaîne de sauvetage suisse formulé par l'Interassociation de sauvetage (IAS) dans sa « Vision du système de secours suisse 2034 ».

Développement dans le cadre d'un réseau coopératif

À l'image des équipes d'intervention sur le lieu du sinistre, de nombreux partenaires issus de différentes institutions participent également au projet SEDH. La Rega est le donneur d'ordre et assure le financement initial. L'entreprise sureVIVE AG agit en tant que développeur, fournisseur et opérateur de la plateforme de la première heure. Du côté de l'industrie, des fournisseurs renommés dans les domaines de la gestion des interventions, des solutions d'alerte et de la communication opérationnelle participent au sous-projet « Architecture ». Dans le sous-projet « Utilisateurs », outre la Rega, le SAS et d'autres partenaires, trois cantons pilotes sont également impliqués : le canton des Grisons, qui a été le premier canton à charger le SAS de mettre en place un dispositif FR+ et qui dispose donc d'une longue expérience avec les applications SAS. Le canton de Saint-Gall, qui apporte une grande expérience en matière de coopération interinstitutionnelle et intercantonale dans le domaine du sauvetage aquatique, où coopèrent les plongeurs de la police cantonale de Saint-Gall, les forces de la section SLRG Mittelhaut et les spécialistes du canyoning du Secours alpin de Suisse orientale (ARO). Enfin, le canton du Tessin, qui a connu une profonde tristesse lors des violentes intempéries de 2024 dans le Val Mesolcina, la vallée de la Maggia et le Val Bavona, mais qui a également pu acquérir une vaste expérience pratique en matière de coopération intercantonale et interorganisationnelle entre les services de secours, qui se traduira désormais par de précieuses contributions au SEDH.

La collaboration au sous-projet « Utilisateurs » est possible

Tout comme pour la mobilisation des forces en cas d'événement, le nombre de personnes, d'entreprises, d'organisations et de cantons engagés dans le projet SEDH continuera d'augmenter de manière entièrement prévue, comme l'explique Martin Thalmann : « Les personnes intéressées qui souhaitent collaborer au projet SEDH, en particulier au sein du groupe < Utilisateurs >, sont invitées à nous contacter. » Enfin, le projet vise à bénéficier d'une large base afin d'être accepté et utilisé à l'échelle nationale. C'est pourquoi, selon Martin Thalmann, il est également envisagé qu'à partir d'un certain stade, le SEDH soit géré, financé et développé par un organisme responsable qui reste à créer. Au profit des organisations participantes, et des personnes qui se trouvent en situation d'urgence en Suisse et qui doivent être aidées dans le cadre d'un réseau coopératif.

Les organisations intéressées peuvent obtenir de plus amples informations auprès de l'entreprise sureVIVE AG sur le site Internet www.sedh.ch, par e-mail à l'adresse connect@sedh.ch ou par téléphone au 091 646 29 04.

Una piattaforma per lo scambio di informazioni nel settore del salvataggio a livello nazionale

Quando le forze di salvataggio si mobilitano per un'operazione si tratta spesso di un «evento cooperativo», in cui esperti di varie organizzazioni agiscono simultaneamente, sovente da regioni o anche cantoni diversi. Affinché tutti dispongano sempre di tutte le informazioni rilevanti, sureVIVE AG ha lanciato insieme a dei partner il progetto «Swiss Emergency Data Hub» (SEDH).



» La Rega opera in tutta la Svizzera e collabora costantemente con le forze locali di altre organizzazioni (di salvataggio). L'interazione tra queste forze viene praticata regolarmente (come mostrato qui). Il SEDH segna un'altra pietra miliare nel percorso verso una cooperazione ancora migliore, al di là dei confini organizzativi e operativi.

Se capita un incidente in Svizzera, le forze di intervento delle organizzazioni di sicurezza e salvataggio accorrono sempre sul posto per fornire aiuto, soccorso, effettuare operazioni di recupero o estinzione. In genere, ogni evento (da un principio d'incendio in cucina ai grandi eventi sovraregionali, come le catastrofi naturali intercantionali) richiede la cooperazione delle forze di svariate organizzazioni. Ad esempio, pompieri, servizio medico e polizia, ma anche soccorritori stradali, aerei, alpini, in altezza, in pro-

fondità e idrici, nonché First Responder (FR), cani da ricerca in superficie, protezione civile e dalle catastrofi.

Ogni organizzazione della famiglia a girofaro blu svizzera ha finalità specifiche, punti di forza individuali, dispone di esperti specializzati e degli strumenti adatti. Dall'unione di queste forze nasce una potente collaborazione, che consente di reagire con prestazioni specifiche per l'evento, in modo rapido, efficiente, garantendo la massima qualità e sicurezza.



» Le applicazioni «MOMENTUM PRO» e «ARMC», così come la comunicazione di gruppo dinamica tramite Threema, hanno dimostrato la loro efficacia nella collaborazione tra Rega, SAS, CAS e First Responder, come si vede qui durante la valanga del 26 dicembre 2019 ad Andermatt. Ora il sistema sarà ulteriormente sviluppato per divenire il sistema nazionale SEDH.

Esempio: valanga in un'area per sport invernali

Un ottimo esempio è dato da una (ipotetica) valanga in un comprensorio sciistico. Indipendentemente dal tipo di segnalazione pervenuta (tramite una persona privata, un operatore dell'impianto di risalita o un pattugliatore sciistico, l'allarme ricevuto dalla centrale operativa della Rega tramite il numero 1414, attiva una procedura a cascata, coinvolgendo forze di intervento di varie organizzazioni: servizi di salvataggio sulle piste, specialisti, conduttori di cani da valanga e stazioni di salvataggio del Soccorso Alpino Svizzero (SAS), polizia, servizio medico e la Rega stessa. A queste si aggiungono istituzioni civili, come società commerciali di elicotteri che effettuano operazioni di trasporto o, in taluni casi, First Responder o Peer.

Cooperazione e comunicazione sono la base per il successo

Affinché la collaborazione interorganizzativa e, non di rado, anche interregionale sia diretta e coordinata in modo ottimale, un fattore è fondamentale per la buona riuscita delle operazioni: avere un quadro comune della situazione, basato su informazioni e dati forniti in tempo reale e una soluzione di comunicazione sempre accessibile a tutti.

Nell'esempio della valanga summenzionato, in cui la velocità dell'aiuto costituisce un fattore critico, devono essere impiegati in modo rapido e mirato risorse umane e materiali. Avere un quadro uniforme della situazione consente, ad esempio, di caricare le forze di intervento a bordo degli elicotteri in modo efficiente, stimare i tempi di volo e valutare la situazione presso il cono di valanga. Inoltre, nel quadro comune della situazione, la visibilità degli elicotteri ha ripercussioni positive in termini di sicurezza di volo.

La prima fase nelle operazioni è decisiva per la gestione complessiva dell'evento quanto quelle successive, che si accompagnano ad un «potenziamento» di risorse e strumenti. Pertanto, persone, veicoli ed elicotteri vanno integrati nel sistema in base alla situazione, sempre in modalità manuale o automatizzata, con elevata disponibilità e indipendentemente dall'hardware.

Quadro della situazione in tempo reale e direzione d'intervento grazie alle soluzioni di sureVIVE

Una soluzione comprovata per l'esempio proposto esiste dal 2021 con l'«Alpine Rescue Mission Control» (ARMC). Questa si basa sullo strumento SaaS «Momentum PRO» e serve a dare l'allarme, dirigere le operazioni e a fornire un quadro della situazione in caso di operazioni aeree e via terra (vedi anche GIROFARO 04-2024). Il sistema è stato sviluppato e gestito da sureVIVE AG, con sede a Mendrisio. «In una situazione di emergenza nell'area alpina che richieda l'intervento del SAS, le sue forze di salvataggio e, se necessario,

altre forze di salvataggio, come i soccorritori sulle piste, vengono chiamate mediante «ARMC». L'allarme viene dato al numero di emergenza sanitaria 144 o a quello di allarme della Rega 1414, che in casi simili assume spesso anche la coordinazione dell'operazione», spiega il CEO di sureVIVE, Georg Hauzenberger.

La chiamata delle forze di intervento dopo l'allarme può quindi avvenire in modo completamente automatico secondo il principio del «Next-Best», grazie ad un algoritmo flessibile e intelligente. Oppure, se necessario, può essere effettuata manualmente.

Subito dopo la fase di allarme e chiamata, la soluzione si tramuta in sistema di direzione dell'operazione e di rapporto sulla situazione, con cui è possibile monitorare, informare e dirigere le forze di intervento dispiegate. «Possono poi essere coinvolte anche altre forze nella fase di potenziamento», spiega Georg Hauzenberger. «Grazie al quadro della situazione in tempo reale su base cartografica, tutti hanno una visione perfetta in qualsiasi momento e per l'intera durata dell'operazione.»

Inoltre, in termini di ecosistema dei migliori sistemi informatici, da «Momentum PRO» e anche da «ARMC», tutti possono creare automaticamente dei gruppi nell'app di comunicazione Threema, sicura e conforme alla protezione dei dati. Questi potranno poi essere utilizzati da tutte le forze di intervento coinvolte ai fini di una comunicazione multimediale (vedi anche GIROFARO BLU 04-2025).

La Rega desidera emancipare il comprovato sistema con i partner nel progetto SEDH

Fin dall'inizio, la Rega è stata molto coinvolta nello sviluppo. Questa si avvale del sistema nella propria centrale operativa per attivare, coordinare, supportare e dirigere operazioni di emergenza dei soccorritori alpini SAS e dei rispettivi gruppi di First Responder Plus (FR+) e di altre forze di salvataggio, come i soccorritori idrici nella Svizzera orientale. Anche per i servizi di salvataggio sulle piste, il sistema è sempre più impiegato in tutta la Svizzera, con l'obiettivo di integrare tutti i servizi in modo efficiente nella catena di



» Non solo, ma in particolare dopo gli eventi meteorologici estremi del 2024 in Ticino, quando anche la Rega è intervenuta (foto), abbiamo capito quanto sia fondamentale la collaborazione di tutte le forze coinvolte nella catena di salvataggio. In futuro, queste forze potranno condividere informazioni e il quadro della situazione in tempo reale tramite il SEDH, in modo rapido e semplice.

salvataggio e perfino di consentire la richiesta elettronica di elicotteri di salvataggio e, se del caso, di ambulanze.

Dopo aver lavorato ormai per quasi cinque anni con questo sistema su quasi tutto il territorio nazionale, la Rega desidera ampliarlo insieme ai partner a girofaro blu e dell'industria e svilupparlo ulteriormente nel «Swiss Emergency Data Hub». Il sistema dovrà consentire il collegamento di tutte le organizzazioni interessate della famiglia a girofaro blu svizzera, al fine di poter condividere tra di loro le informazioni sull'operazione. «In modo autodeterminato e basato sui ruoli, secondo criteri rigorosi in materia di sovranità e protezione dei dati», come sottolinea Georg Hauzenberger.

Questa l'intenzione dietro al progetto SEDH

L'idea alla base del progetto SEDH è tanto semplice quanto logica. Come organizzazione di soccorso aereo attiva a livello nazionale, la Rega ha sempre operato a livello trans-regionale. Inoltre, agisce sempre in modo interorganizzativo, in collaborazione con le forze di competenza sul luogo dell'intervento. Di conseguenza, la necessità di uno scambio efficiente e sicuro di informazioni e dati oltre i confini istituzionali, regionali e cantonali è fondamentale.

Ad oggi, la Rega, che opera in tutta la Svizzera, si trova ad affrontare due ostacoli principali: la «cecità» spesso indotta da fattori tecnici delle organizzazioni locali rispetto a tutto ciò che accade al di fuori dei propri confini spaziali e organizzativi, spesso definiti in modo ristretto, e il fatto che la Svizzera attualmente non disponga né di una centrale nazionale delle emergenze mediche (SNZ) né di un ecosistema digitale nazionale in grado di fornire informazioni in tempo reale sulle risorse umane e le attrezzature disponibili in caso di incidente, per e da parte di tutte le forze coinvolte in un evento specifico.

Entrambi i fattori influiscono negativamente sulla capacità di sfruttare un quadro della situazione condiviso da tutte le forze di intervento coinvolte in un incidente e di applicare costantemente il principio del «Next-Best» in ogni momento. Per via della struttura frammentata e del federalismo della Svizzera, ci si imbatte in un mosaico di responsabilità, organizzazioni e aree operative, così evolutosi nel corso degli anni. Di conseguenza, lo scambio di informazioni rilevanti dal punto di vista operativo durante le operazioni cooperative risulta spesso macchinoso. I silos informativi sono la norma, così come le interruzioni nella trasmissione di informazioni o dati. Tutto questo è ora destinato a cambiare con lo «Swiss Emergency Data Hub».

Condividere informazioni essenziali, in modo autodeterminato e sicuro

Il sistema è già in fase di sviluppo ed è progettato per raggruppare tutte le informazioni rilevanti in un'unica posizione centrale in caso di incidente, consentendo l'accesso a tutte le organizzazioni coinvolte. Una sfida impor-

te è stata quella di rispettare le rigide normative sulla protezione dei dati e garantire che ogni organizzazione mantenesse il proprio controllo inviolabile e la propria sovranità sui dati. «Il SEDH affronta pienamente entrambi questi problemi», sottolinea il responsabile del programma Martin Thalmann. «I dati vengono trasmessi in streaming sull'hub, ma non archiviati. Inoltre, ogni organizzazione connessa decide autonomamente con chi condividere i dati e quali dati condividere». I dati vengono trasmessi in streaming in base ai ruoli degli utenti, in modo simile a «Momentum PRO». «Ad esempio, è impossibile per un'organizzazione medica condividere dati sensibili dei pazienti con una compagnia di elicotteri privata che fornisce voli di trasporto o per quest'ultima ottenere in alcun modo l'accesso a tali dati sensibili», assicura Martin Thalmann.

Utilizzo delle tecnologie esistenti

Per quanto visionario possa sembrare il progetto SEDH, non richiede una reinvenzione del mondo digitale. Con «Momentum PRO», «ARMC» e la «Comunicazione Dinamica di Gruppo» tramite Threema Work, implementati da sureVIVE e Threema per il SAS, esistono già elementi essenziali e collaudati. A questi si aggiungono soluzioni per la distribuzione delle informazioni. «Anch'esse già esistenti. Le stiamo dunque applicando a SEDH in un nuovo contesto, e con un rigore senza precedenti», rivela Georg Hauzenberger.

L'architettura delle interfacce, invece, ha dovuto essere completamente ripensata, come spiega: «Le classiche connessioni punto-punto avrebbero richiesto un numero molto elevato di interfacce, il che aumentava la complessità operativa e i costi per le organizzazioni a girofaro blu. Puntiamo invece su un'architettura relativa all'evento. Tutto avviene sul SEDH e ogni organizzazione ha pertanto bisogno di una sola interfaccia: quella con l'hub.»

Le interfacce sono attualmente in fase di sviluppo presso rinomati fornitori specializzati svizzeri, come Hexagon, LogObject, Swisscom e sureVIVE. L'obiettivo è che le organizzazioni interessate dovrebbero essere in grado di accedere al SEDH tramite connessioni standardizzate, indipendenti e perfettamente adattate alle soluzioni per la rispettiva centrale di emergenza. «Quando si configura l'interfaccia con l'hub, è quindi possibile definire con precisione quali informazioni debbano essere condivise con quali altre organizzazioni e quali no», spiega Georg Hauzenberger.

Occorre una sola interfaccia per il SEDH

In caso di incidente, le informazioni rilevanti non vengono mai memorizzate sul SEDH, ma piuttosto trasmesse in streaming tramite esso e condivise in base alle rispettive configurazioni di interfaccia. In questo modo, le informazioni generate da un'organizzazione (ad esempio, una centrale delle emergenze mediche cantonale che attiva un'operazione a seguito di un allarme) vengono rese accessibili agli altri attori coinvolti nell'incidente. Questi ultimi ricevono, visualizzano ed elaborano le informazioni, ad esempio, tramite la centrale delle emergenze mediche che invia un'ambulanza, la Rega che invia un elicottero e la rispettiva organizzazione cantonale FR o il SAS che invia un First Responder o un First Responder+. Queste informazioni vengono trasmesse, tramite l'hub, agli altri partner. Tutte le centrali di emergenza coinvolte e le forze di salvataggio sul posto sanno immediatamente che l'ambulanza, la Rega e i First Responder sono in arrivo. Naturalmente, possono anche vedere la loro posizione in tempo reale sulla mappa.

«Ne deriva un quadro dettagliato, dinamico e in tempo reale della situazione.» «Tutti sanno cosa è già stato avviato e fatto, cosa è in corso, chi si trova dove e quali sono i prossimi passi da compiere», spiega Adrian Schindler, portavoce della Rega. «Risorse, azioni e attrezzature diventano trasparenti per tutti. Questo facilita e intensifica il lavoro di squadra, consente decisioni basate sui fatti in meno tempo ed evita richieste di informazioni, malintesi e interpretazioni errate. Di conseguenza, le operazioni cooperative possono essere gestite in modo più rapido, efficiente e sicuro.»

Con tale obiettivo fondamentale, il progetto è specificamente in linea con quello della completa digitalizzazione della catena di soccorso svizzera, formulato dall'Interassociazione di salvataggio (IAS) nella sua «Visione del sistema di soccorso svizzero 2034».

Sviluppo in una rete cooperativa

Seguendo l'esempio dei soccorritori sul luogo dell'incidente, anche numerosi partner di diverse istituzioni sono coinvolti nel progetto SEDH. La Rega è la committente e fornisce il finanziamento iniziale. sureVIVE AG è stata fin dall'inizio la sviluppatrice e fornisce e gestisce la piattaforma. Dal punto di vista industriale, al sottoprogetto «Architettura» hanno aderito rinomati fornitori nei settori della gestione degli incidenti, delle soluzioni di allarme e della comunicazione d'emergenza. E nel sottoprogetto «Utenti», oltre alla Rega con il SAS e altri partner, sono coinvolti anche tre cantoni pilota: il Canton Grigioni, che è stato il primo cantone ad



» Georg Hauzenberger, CEO di sureVIVE (in foto con Stefano Doninelli, «padre» di «MOMENTUM» e CINO di sureVIVE): «È necessario abbattere i confini che impediscono alle forze di intervento di organizzazioni di salvataggio cooperanti di avere la stessa visione sulla situazione. Il progetto SEDH porta alla 'Democratizzazione del salvataggio', a beneficio di tutti i soggetti coinvolti.»

incaricare il SAS di realizzare un sistema FR+ e vanta quindi un'esperienza pluriennale con le app SAS; il Canton San Gallo, che ha una notevole esperienza nella cooperazione oltre i confini istituzionali e cantonali nel campo del salvataggio in acqua, dove collaborano i sommozzatori della polizia cantonale di San Gallo, la Società svizzera di salvataggio (SLRG) Medio Reno e gli specialisti del canyoning del Soccorso alpino della Svizzera orientale (ARO); il Canton Ticino, che ha sofferto molto durante i gravi eventi meteorologici del 2024 in Mesolcina, Valle Maggia e Val Bavona, ma ha anche maturato una vasta esperienza pratica nella cooperazione intercantionale e interorganizzativa tra le forze di salvataggio, portando ora preziosi contributi al SEDH.

Cooperare nel sottoprogetto «Utenti» è possibile

Analogamente al potenziamento delle risorse in caso di emergenza, il numero di individui, aziende, organizzazioni e cantoni coinvolti nel progetto SEDH continuerà a crescere, un aspetto del tutto pianificato, come spiega Martin Thalmann: «Chiunque sia interessato a collaborare al progetto SEDH, in particolare al gruppo degli «Utenti», è invitato a contattarci.» D'altronde, il progetto mira a ottenere un ampio sostegno per promuoverne l'accettazione e l'utilizzo a livello nazionale. Secondo Martin Thalmann, si prevede anche che, a un certo punto, il SEDH sarà gestito, finanziato e ulteriormente sviluppato da un'organizzazione sponsor ancora da costituire. Ciò andrà a vantaggio delle organizzazioni partecipanti, oltre che delle persone coinvolte in una situazione di crisi in Svizzera che richieda il coinvolgimento di una rete cooperativa.

Le organizzazioni interessate potranno ottenere ulteriori informazioni da sureVIVE AG, sul sito www.sedh.ch, via e-mail all'indirizzo connect@sedh.ch o telefonicamente al numero 091 646 29 04.

Technologie, die Sicherheit stärkt. IT-Kompetenz für Blaulichtorganisationen



Computacenter in der Schweiz unterstützt seit vielen Jahren sicherheitskritische Organisationen dabei, ihre IT-Umgebungen stabil, sicher und einsatzbereit zu halten. Schweizweit begleiten wir Behörden über den gesamten Technologie-Lebenszyklus mit internationaler Expertise und lokaler Nähe, die in dynamischen Einsatzsituationen den entscheidenden Unterschied macht.

Ein besonderer Fokus liegt auf modernen Arbeitsplatz- und Geräteinfrastrukturen, die im Blaulichtumfeld unverzichtbar sind. Wir sorgen dafür, dass Einsatzkräfte jederzeit auf leistungsfähige und sichere Endgeräte zugreifen können, vom Notebook bis zu mobilen Geräten, die für Rapportierung, Dokumentation und Lageeinschätzung essenziell sind.

Viele Behörden setzen iPhone und iPad als standardisierte Arbeitsmittel ein. Als einziger «Apple Premium Business Partner» in der Schweiz verfügen wir über ausgewiesene Expertise und direkten Zugang zu Apple-Ressourcen. Wir unterstützen Sie dabei mit zertifizierten Spezialisten, effizienten Serviceprozessen und einem klar strukturierten Geräte-Lifecycle.

Ein eindrückliches Beispiel dafür ist die erfolgreiche Umsetzung einer mehrjährigen iPhone-Beschaffung für eine Schweizer Polizeiorganisation: von der sorgfältigen Planung über die termingerechte Lieferung und Zubehörberatung bis zur strukturierten Rücknahme der Altgeräte. Durch produktnahe Dienstleistungen, etwa das fachgerechte Anbringen von Schutzgläsern, konnten die Geräte den Einsatzkräften unmittelbar einsatzbereit übergeben werden.

Auch im Bereich künstliche Intelligenz begleiten wir Behörden verantwortungsvoll und zukunftsorientiert. Wir

entwickeln sichere KI-Governance-Modelle, implementieren Microsoft-Copilot-Lösungen und unterstützen bei Text- und Bildanalyse, Prozessautomatisierung oder Edge-AI für Entscheidungen direkt am Einsatzort. Viele Organisationen benötigen dabei höchste Verfügbarkeit und volle Kontrolle über sensible Daten. Deshalb ergänzen wir KI-Lösungen gezielt durch moderne On-Prem- und Hybrid-Modelle, die kritische Systeme auch bei eingeschränkter Konnektivität zuverlässig betreiben. Gleichzeitig stärken wir die digitale Souveränität unserer Kunden, indem wir EU-konforme Datenhaltung, sichere Private- und Hybrid-Cloud-Optionen sowie vollständig kontrollierbare Infrastrukturmöglichkeiten ermöglichen. So bleibt KI nutzbar, wirkungsvoll und jederzeit unter der Kontrolle der Behörden.

Das Ergebnis: eine verlässliche, langfristige Partnerschaft, die operative Sicherheit mit effizientem Lifecycle-Management verbindet. Wir helfen unseren Kunden, ihre IT-Infrastruktur zu beschaffen, weiterzuentwickeln und zu betreiben für eine digitale Transformation, die Menschen und ihre Mission erfolgreich macht.

Kontakt:

Unsere Spezialisten beraten Sie persönlich, individuell und mit tiefem Verständnis für die Anforderungen von Blaulichtorganisationen. Gemeinsam schaffen wir eine IT, auf die man sich verlassen kann.



Auch Banknoten haben Fingerabdrücke: Auf den Spuren inkriminierter Geldscheine

Die Frankfurter Elephant & Castle IP GmbH hat entwickelt, worauf alle Strafverfolgungsbehörden seit Erfindung der Banknote händeringend gewartet haben: eine Methode zur Nachverfolgbarkeit des Weges einzelner Geldscheine. Das revolutioniert die Möglichkeiten bei Fahndung und Aufklärung.



» Können Fahndungs- und Strafverfolgungsbehörden den Weg von Bargeld nachverfolgen, erweitert das die Möglichkeiten zur Aufklärung von Straftaten immens.

Manchmal sind Herausforderungen klar wie ein Bergsee und Lösungsansätze zwar offensichtlich, aber in der Praxis unfassbar aufwendig und komplex. Dann wird es schwierig – so wie bislang bei der praktischen Nachverfolgung inkriminierter oder zumindest verdächtiger Banknoten.

Letztere gibt es – alle, die BLAULICHT 03-2025 gelesen haben, wissen es – in der Schweiz seit 200 Jahren. Und alle Geldscheine sind seit der ersten Serie mit einer alphanumerischen Identifikationsnummer versehen. Diese macht – in Kombination mit dem Notenwert und der Art der Währung – jede Banknote unverwechselbar. Zudem erlaubt sie eindeutige Rückschlüsse zu Produktionszeit und Produktionsort (Land und Druckerei), bisweilen sogar zum individuellen Druckbogen, der zu ihrer Herstellung diente. Folgt die Identifikationsnummer einer Banknote zugleich einer mathematischen Logik, ist via Prüfziffernberechnung auch eine Echtheitsprüfung möglich.

Der Fingerabdruck jedes Geldscheins

So weit und durchdacht das althergebrachte System des alphanumerischen Fingerabdrucks jeder Banknote ist, so begrenzt blieb dessen effektiver praktischer Nutzen für Ermittler und Strafverfolgungsbehörden – zumindest bisher. Denn zwar werden die Identifikationsnummern bei der Herstellung und bei der Erstaussgabe von Geldscheinen moderner Währungen erfasst und dokumentiert. Doch sobald die Banknoten in den Umlauf wechseln, schert sich eigentlich niemand mehr um deren Nummern. Banken erfassen nicht, welche Scheine sie bei Schalterbezügen in welcher Filiale zu welchem Zeitpunkt an wen aushändigen. Ebenso landen viele Geldscheine in Bankomaten, ohne dass zuvor deren Nummern erfasst worden wären. Und freilich kommen weder Einzelhändler noch Gastronomen auf die Idee, die Identifikationsnummern der Geldscheine zu notieren, die über die Theke wandern – in welche Richtung auch immer. Von uns Privatpersonen reden wir hier erst gar nicht – und das aus Krimis bekannte «Registergeld», also Scheine, deren Nummern erfasst wurden, obwohl Kriminelle «keine Million in kleinen, nicht nummerierten Scheinen» verlangt haben, ist ebenfalls pure Hollywood-Fiktion.

Bargeld ist der Liebling Krimineller ...

So kommt es, dass Bargeld seit seiner Erfindung der Liebling Krimineller ist – und zunehmend in Verruf gerät. «Papiergeld ist immens teuer – und die Wurzel allen Übels», behaupten Bargeld-Kritiker. Doch ist das tatsächlich so?

Die Antwort von Gerrit Stehle, Managing Partner der Elephant & Castle IP GmbH, auf diese Frage mag verwundern. Denn er ist vom System Bargeld überzeugt: «Banknoten sind ein seit Jahrhunderten bewährtes Zahlungsmittel. Leicht handhabbar, grundlegend sicher und eingebunden in ein hervorragend funktionierendes, international bewährtes Kreislaufsystem.»

Schlecht ist aus seiner Sicht einzig, dass der hohe Stellenwert der Identifikationsnummer viel zu lange ignoriert wurde – mangels Technologien, die deren effiziente Nutzung ermöglichen würden. «Die Herausforderung ist klar: Wer Kriminellen das Handwerk legen will, muss die Wege von Banknoten nachvollziehen können. Eine grundlegende Lösung dafür gibt es: die Identifikationsnummer, dank der jeder Geldschein identifiziert und damit nachverfolgt werden kann. Allerdings hatte bis vor kurzer Zeit niemand eine zündende Idee, mithilfe welcher Technologien dies ebenso einfach wie schnell realisiert werden kann», sagt Gerrit Stehle.

... bis Gerrit Stehle und sein Team eine zündende Idee hatten

Vor knapp einem Jahrzehnt nahmen er und sein Team sich dieses Problems an – und entwickelten eine patentierte Methode, die den Strafverfolgungsbehörden revolutionär neue Möglichkeiten beschert. «Wir machen die Geldströme in der Eurozone rechtsstaatlich sicht-, nutz- und nachvollziehbar», sagt Gerrit Stehle. «Mithilfe einer unternehmens-eigenen Software, einer riesigen Datenbank und in enger Kooperation mit diversen, im regulären Bargeldsystem aktiven Partnern, namentlich Werttransportunternehmen (WTU) und Cash Center. Dabei bleiben Datenschutz und Persönlichkeitsrechte gewahrt, die Anonymität des Bargeldes wird nicht grundlegend tangiert und natürlich differenzieren wir die digitalen von den physischen Geldströmen. Zudem unterstützt das System die bei Polizei und Strafverfolgungsbehörden bereits in Nutzung stehenden Software-Lösungen.»

Klingt verlockend – doch welcher Aufwand muss dazu betrieben werden? «Der ist überschaubar», betont Gerrit Stehle.



» Konkreter Use Case: Dank der automatisierten Identifikationsnummernerfassung wird die Bargeldlogistik markant sicherer.

So funktioniert das digitale Bargeld-Tracking

In einem ersten Schritt werden die Identifikationsnummern möglichst vieler Geldscheine durch Geldtransportunternehmen erfasst – mithilfe moderner Geldzähl- und Geldprüfgeräte, wie sie auch Bundesbehörden, Banken sowie häufig auch (grössere) Einzelhandelsunternehmen bereits seit Jahren nutzen. «Die besten dieser Geräte können Banknoten diverser Währungen nicht nur zählen, sortieren und via OCR-Messungen (Optical Character Recognition) authentifizieren, sondern zugleich auch deren Identifikationsnummern erfassen und speichern – mit einem Tempo von bis zu 1'000 Scheinen pro Minute», erklärt Gerrit Stehle. «Wichtig dabei ist, dass bei der Nummernerfassung keine Fehler passieren respektive Probleme, etwa verschmutzte Geldscheine, sauber erkannt werden», betont er. Daher haben er und sein Team unzählige auf dem Markt verfügbare Geräte getestet – mit je 10'000 Banknoten. «Wer wissen will, welche dabei gut und welche weniger gut abgeschnitten haben, darf uns gerne kontaktieren, dann liefern wir die Testergebnisse», so Stehle.

Im zweiten Schritt wandern die erfassten Identifikationsnummern – vergleichbar mit Fingerabdrücken – in eine Datenbank. «Suchen nun Ermittlungs- oder Strafverfolgungskräfte nach bestimmten Scheinen, können sie diese – einmal als Vertragspartner registriert – in unserer unternehmens-eigenen Datenbank suchen. Bei Treffern erhalten sie einen stummen Alarm – und sehen beispielsweise, ob die Scheine schon einmal in anderem Zusammenhang behördlich interessant waren (z. B. Betäubungsmittel-Testkäufe, Lösegeldzahlungen, Einzeltrick oder Roaming-Scam-Betrügereien, Bankomatsprengung etc.). Zudem können sie Informationen dazu erhalten, wann und wo die Banknoten gedruckt wurden, ob sie in jüngerer Vergangenheit in Umlauf waren oder gehortet wurden, welchem typischen <Ländermix> ihre Durchmischung entspricht und Weiteres mehr», erläutert Gerrit Stehle.

Mit den dabei gewonnenen Informationen können wichtige ermittlungstaktische Fragen beantwortet werden, wie Gerrit Stehle anhand anonymisierter Beispiele aus der Praxis aufzeigt.

Harmloser Sammler oder ein «Cash Mule»?

An einer innereuropäischen Grenze findet der Zoll bei einer Person 80'000 Euro in bar. Die Person sagt, sie habe in Spanien ein Sammlerstück erwerben wollen und der Verkäufer habe auf Barzahlung bestanden. Vor Ort habe sich das Objekt der Begierde aber als zweifelhaft erwiesen, weshalb der Kauf geplatzt sei – und das aus Deutschland bereits bei der Anreise mitgeführte Geld wieder zurückgebracht werde. «In so einem Fall hatten die Beamten bisher wenig Prüfmöglichkeiten», sagt Stehle. «Erfassen sie aber die Nummern der Banknoten, finden wir für sie heraus, wo diese ursprünglich produziert wurden. Das wiederum erlaubt Rückschlüsse auf deren tatsächliche Herkunft. Denn der prozentuale Anteil spanischer Euro-Banknoten im Umlauf ist in Spanien naturgemäss viel höher als in Deutschland. Läge der Wert beispielsweise im einstelligen Prozentbereich, würde das die Behauptung der Person stärken. Andererseits wäre bei einem sehr hohen Prozentsatz ein begründeter Anfangsverdacht gegeben, dass die Person möglicherweise ein <Money Mule> ist.»

Unwissender Erbe oder fieser Romance Scammer?

Ein anderes Beispiel: Nach mehreren Romance-Scam-Betrugsfällen setzen Fahnder eine verdächtige Person fest. Unter einer losen Diele in deren Keller finden sie knapp 55'000 Euro Bargeld in unterschiedlichen Couverts. Der Verdächtige behauptet, diese kenne er nicht. Die müsse sein vor acht Jahren verstorbener Vater, von dem er das Haus geerbt hat, dort versteckt haben. Die Polizei hegt Zweifel und lässt die Identifikationsnummern der Scheine prüfen. Dabei stellt sich heraus: Die Banknoten waren allesamt in den vergangenen Wochen und Monaten in Zirkulation, können also definitiv nicht jahrelang im Keller gelegen haben. Zudem wurden genau 9'000 Euro des verdächtigen Geldes in den vergangenen fünf Tagen in Tranchen bezogen – an ein und demselben Bankomaten, bei der Hausbank einer 55-jährigen Witwe. Diese gehört, wie weitere Ermittlungen belegen, ebenfalls zum Opferkreis des Betrügers.

«Auch bei Einzeltrick-Betrugsfällen kann eine Überprüfung der Identifikationsnummern von bei Verdächtigen aufgefundenen Banknoten wichtige Hinweise liefern», verrät Gerrit Stehle. «Denn gerade hier tritt in signifikant hohem Mass altes Geld in Erscheinung – und wir können anhand der Identifikationsnummern belegen, wo und wann Banknoten produziert wurden.»

» Würden Banken die Identifikationsnummern aller Geldscheine, die sie in ihre Bankomaten laden, erfassen, könnten bei Bankomatsprengungen erbeutete Banknoten nachverfolgt werden.





» Da die Identifikationsnummer auch das Alter von Geldscheinen enthüllt, kann mit ihrer Hilfe zwischen aktuell umlaufendem Geld und «Matratzenscheinen» unterschieden werden.

Mörder und Bankräuber oder Glückspilz?

Ein dritter Fall: In einer ländlichen Gemeinde geschieht ein Raub. Der Täter – mit markanter Narbe an der Stirn – erbeutet rund 150'000 Euro. Der Fall bleibt ungelöst – bis Zivilfahnder zwölf Jahre später einem anonymen Hinweis folgend einen Verdächtigen ins Visier nehmen. Dieser hat eine auffällige Narbe an der Stirn – und in seiner Wohnung finden die Fahnder in diversen Verstecken mehr als 80'000 Euro Bargeld. Der Mann beteuert seine Unschuld, behauptet, das Geld habe er vor zwei Jahren im Casino gewonnen. Den Banken traue er nicht, weshalb er es zu Hause hortet. Für die Staatsanwaltschaft ist der Fall klar, doch der Pflichtverteidiger veranlasst eine Analyse der Identifikationsnummern der Banknoten. Diese belegt, dass die Banknoten erst zwischen fünf und neun Jahre alt sind – also zum Zeitpunkt des Banküberfalls noch gar nicht existierten. Resultat: Freispruch!

Drei Beispiele, die zeigen, wie wertvoll die Nachverfolgbarkeit von Banknoten für Ermittlung und Strafverfolgung sein kann – und Gerrit Stehle könnte viele weitere nennen. Denn die Technologie wurde bereits in mehr als 300 Strafverfahren eingesetzt – unter anderem auch bei sogenannten «Hawala»-Banking-Fällen, die der Geldwäsche oder der Terrorfinanzierung dienen.

Wertvoll auch für Einzelhändler und für clevere Banken-Services

Neben Fahndung und Strafverfolgung können auch regelmässig mit grossen Bargeldmengen befasste Unternehmen profitieren – und Banken ihren Kunden völlig neue Services anbieten.

«Einzelhändler, die viel mit Bargeld arbeiten, zählen dieses, packen es in Transportbehälter, machen eine Voranmeldung – und ein Dienstleister holt das Geld ab. Würden die Unternehmen beim Zählen der Scheine zugleich deren Nummern erfassen, wüssten sie exakt, welche ihre Scheine waren. Bei Reklamationen, etwa wegen drei angeblichen <falscher Fünfiger> im Behälter, könnten sie belegen, ob diese wirklich von ihnen stammen oder erst nachträglich

von Dritten im Tausch gegen echte Fünfigernoten untergemischt wurden», zeigt Gerrit Stehle auf.

Banken wiederum könnten ihren Kunden bei grösseren oder ungewöhnlichen Bargeldbezügen anbieten, die Identifikationsnummern der Scheine zu erfassen und auf einem USB-Stick abzuspeichern. «In Fällen von Erpressung, Betrug, Diebstahl oder anderweitigem Verlust könnten die Geldscheine nachverfolgt werden», sagt Gerrit Stehle. «Sobald die Scheine bei einem Geldtransportunternehmen erfasst werden, gibt das System Alarm. Da zugleich die Nummer der Geldbombe bekannt ist, in der sie enthalten war, ist klar, woher sie stammen. So wüssten die Ermittler zeitnah, wo sie nach weiteren Spuren der

Täter suchen sollten. Dasselbe geschieht, wenn die Täter das Geld irgendwo einzahlen. Auch dann explodiert die <digitale Farbbombe>.»

Und natürlich rät er allen Banken eindringlich, die Identifikationsnummern aller Scheine, die in Bankomaten geladen werden, zu erfassen: «Die digitale Farbbombe schützt die Banknoten – und ermöglicht bei einer Bankomatsprengung ein schnelles und effektives Tracking.»

Technologie ist gerichtsverwendbar

Die für die Gerichtsverwertbarkeit der Methode nötige Prüfung der Amtswege verlief laut Gerrit Stehle ebenso positiv wie Prüfungen hinsichtlich des Daten- und Persönlichkeitsschutzes. «Alle Daten werden auf zertifizierten, speziell gesicherten und revisionssicheren Servern in Deutschland gespeichert und können optional auf gängige Infrastrukturen wie Bundesserver, Sovereign Clouds oder lokale Rechenzentren von Sicherheitsbehörden zu 100 Prozent gespiegelt werden», betont er. «So können Behörden auf sicherem Weg auf ihre Bedürfnisse abgestimmte Datensätze anlassbezogen abrufen.» Zudem würden keinerlei personenbezogene Daten erfasst, da die Geldtransporteure in aller Regel Firmen betreuen – und keine natürlichen Personen.

Bald auch in der Schweiz verfügbar?

Neben Transparency International, ausgewählten Generalstaatsanwaltschaften und einer Vielzahl deutscher Strafverfolgungsbehörden sind bereits ausländische Sicherheitsbehörden auf die deutsche Innovation aufmerksam geworden – auch aus der Schweiz, wo Gespräche mit wichtigen Stakeholdern laufen, wie Gerrit Stehle verrät.

Zudem entwickelt sein Unternehmen aktuell in Kooperation mit der Schweizer Spezialistin OVD KINEGRAM AG mit dem «BANKNOTE SCANNER» (siehe Artikel in der Rubrik «Test & Technik» dieser Ausgabe) eine App, mit der auch im mobilen Einsatz Banknoten gezählt und deren Identifikationsnummern erfasst werden können – schnell, einfach und zuverlässig.

Les billets de banque ont également des empreintes digitales : Sur les traces des billets suspects

L'entreprise Elephant & Castle IP GmbH, basée à Francfort, a développé ce que toutes les autorités judiciaires attendaient avec impatience depuis l'invention du billet de banque : une méthode permettant de retracer le parcours de chaque billet. Cela révolutionne les possibilités en matière d'enquête et d'élucidation.



» Dans les cas d'arnaque au petit-fils, les auteurs volent souvent des billets de banque très anciens (conservés à domicile). Le numéro d'identification d'un billet de banque permet de déterminer son âge. Il est ainsi possible de tirer des conclusions.

Parfois, les défis sont aussi clairs qu'un lac de montagne et les solutions semblent évidentes, mais elles sont en réalité extrêmement coûteuses et complexes à mettre en œuvre. C'est alors que les choses se compliquent, comme cela a été le cas jusqu'à présent pour le suivi pratique des billets de banque frauduleux ou au moins suspects.

Les billets existent en Suisse depuis 200 ans, comme le savent déjà les lecteurs de l'édition 03-2025 de BLAULICHT. Et depuis la première série, tous les billets de banque sont pourvus d'un numéro d'identification alphanumérique. Combiné à la valeur faciale et au type de monnaie, ce numéro rend chaque billet de banque unique. Il permet également de déterminer avec certitude la date et le lieu de production (pays et imprimerie), voire parfois la feuille d'impression individuelle qui a servi à sa fabrication. Si le numéro d'identification d'un billet de banque suit une logique mathématique, il est également possible de vérifier son authenticité à l'aide d'un calcul de chiffre de contrôle.

L'empreinte digitale de chaque billet de banque

Aussi bien pensé que soit le système traditionnel d'empreinte alphanumérique de chaque billet de banque, son utilité pratique pour les enquêteurs et les autorités judiciaires est restée limitée, du moins jusqu'à présent. En effet, les numéros d'identification sont enregistrés et documentés lors de la fabrication et de la première émission des billets de banque des monnaies modernes. Mais dès que les billets sont mis en circulation, personne ne se soucie plus vraiment de leurs numéros. Les banques n'enregistrent pas les billets qu'elles remettent lors des retraits au guichet, ni l'agence qui les remet, ni le moment de la remise et ni la personne qui les reçoit. De même, de nombreux billets sont distribués par les distributeurs automatiques sans que leurs numéros aient été préalablement enregistrés. Et bien sûr, ni les détaillants ni les restaurateurs n'ont l'idée de noter les numéros d'identification des billets de banque qu'ils encaissent ou qu'ils remettent. Sans parler des particuliers. Et « l'argent enregistré » que l'on voit dans les films policiers, c'est-à-dire les billets dont les numéros ont été enregistrés, alors que les criminels ont réclamé « un million en petites coupures non numérotées », relève également de la pure fiction hollywoodienne.

L'argent liquide est la cible des criminels ...

C'est ainsi que depuis son invention, l'argent liquide est devenu la cible des criminels et qu'il est de plus en plus discrédité. « Le papier-monnaie est extrêmement coûteux et la source de tous les maux », affirment les détracteurs de l'argent liquide. Mais est-ce vraiment le cas ?

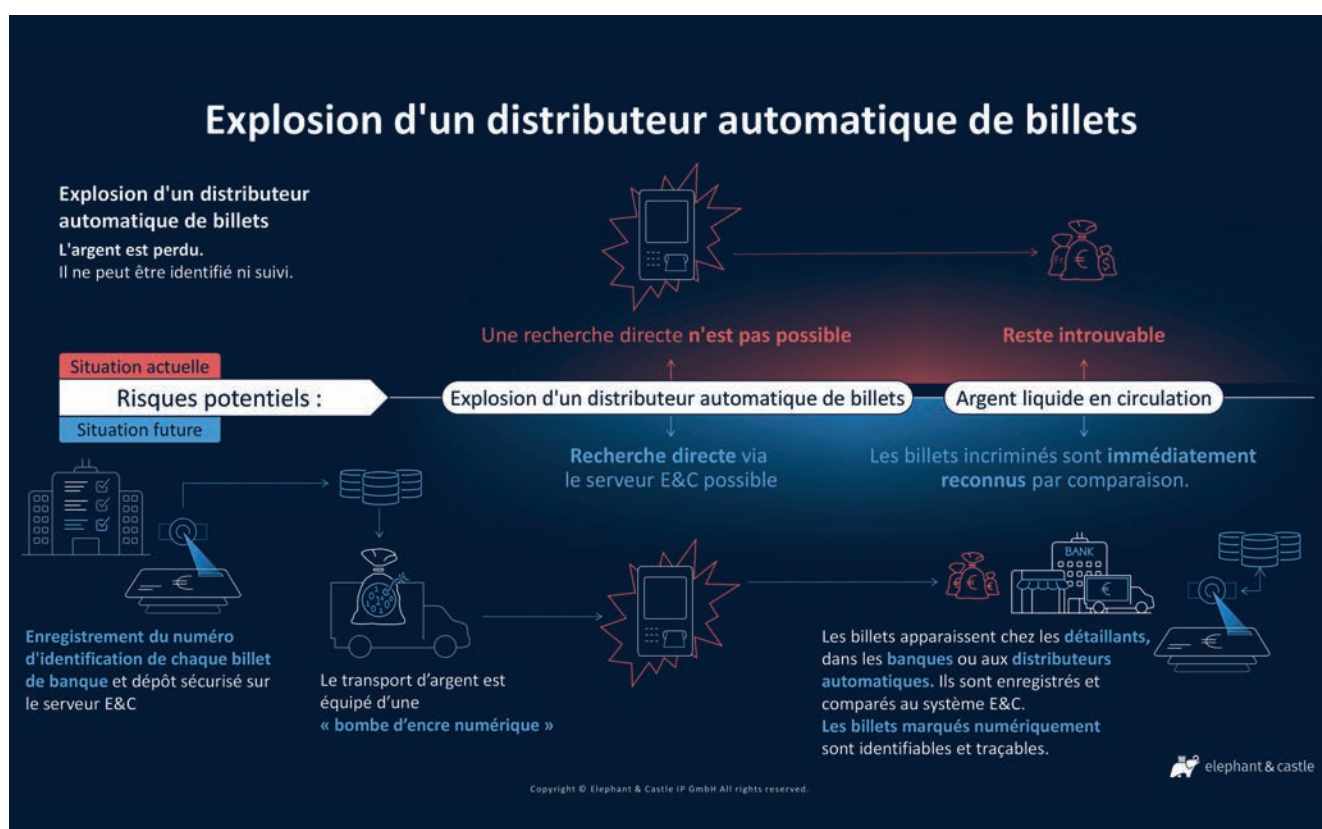
La réponse de Gerrit Stehle, associé gérant d'Elephant & Castle IP GmbH, à cette question peut surprendre. Il est en effet convaincu par le système de l'argent liquide : « Les billets de banque sont un moyen de paiement qui a fait ses preuves depuis des siècles. Ils sont faciles à manipuler, fondamentalement sûrs et intégrés dans un système de circulation qui fonctionne parfaitement et qui a fait ses preuves à l'échelle internationale. »

Selon lui, le seul point négatif est que l'importance du numéro d'identification a été ignorée pendant trop longtemps, en raison du manque de technologies permettant son utilisation efficace. « Le défi est clair : Pour mettre fin aux activités des criminels, il est nécessaire de pouvoir retracer le parcours des billets de banque. Il existe une solution fondamentale à ce problème : le numéro d'identification, qui permet d'identifier chaque billet de banque et donc de le suivre. Mais jusqu'à récemment, personne n'avait trouvé l'idée lumineuse permettant de trouver la technologie qui permettrait de suivre les billets de manière simple et rapide », explique Gerrit Stehle.

Jusqu'à ce que Gerrit Stehle et son équipe trouvent cette idée ingénieuse

Il y a près de dix ans, lui et son équipe se sont penchés sur ce problème et ont développé une méthode brevetée qui offre aux autorités judiciaires de nouvelles possibilités révolutionnaires. « Nous rendons les flux financiers dans la zone euro visibles, exploitables et traçables dans le respect de l'État de droit », explique Gerrit Stehle. « Et ce, grâce à un logiciel développé en interne, à une immense base de données et à une étroite collaboration avec divers partenaires actifs dans le système monétaire traditionnel, à savoir les transporteurs de fonds (WTU) et les centres de traitement des espèces. La protection des données et les droits des personnes sont préservés, l'anonymat de l'argent liquide n'est pas fondamentalement affecté et nous faisons bien sûr la distinction entre les flux financiers numériques et physiques. De plus, le système prend en charge les solutions logicielles déjà utilisées par la police et les autorités judiciaires. »

Cette idée est séduisante, mais quel effort financier demande-t-elle ? « L'effort reste raisonnable », souligne Gerrit Stehle.



» Cas d'utilisation concret : L'enregistrement automatisé des numéros d'identification permet de suivre les billets de banque volés lors d'explosions de distributeurs automatiques.

Voici comment fonctionne le suivi numérique des espèces

Dans un premier temps, les numéros d'identification du plus grand nombre possible de billets sont enregistrés par les sociétés de transport de fonds à l'aide d'appareils modernes de comptage et de vérification des billets, tels que ceux utilisés depuis des années par les autorités fédérales, les banques et les (grandes) entreprises de vente au détail. « Ces appareils les plus performants peuvent non seulement compter, trier et authentifier les billets de banque de différentes devises à l'aide de mesures OCR (reconnaissance optique de caractères), mais également enregistrer et stocker leurs numéros d'identification, à une vitesse pouvant atteindre 1 000 billets par minute », explique Gerrit Stehle. « Il est important que la saisie des numéros se fasse sans erreur et que les problèmes, tels que les billets sales, soient correctement détectés », souligne-t-il. C'est pourquoi lui et son équipe ont testé d'innombrables appareils disponibles sur le marché, avec 10 000 billets chacun. « Si vous souhaitez connaître les appareils qui ont obtenu de bons résultats et ceux qui ont obtenu des résultats moins bons, n'hésitez pas à nous contacter, nous vous fournirons les résultats des tests », déclare Gerrit Stehle.

Dans un deuxième temps, les numéros d'identification enregistrés, comparables à des empreintes digitales, sont transférés dans une base de données. « Si les enquêteurs ou les autorités judiciaires recherchent des billets spécifiques, ils peuvent les trouver dans la base de données de notre entreprise, à condition d'être enregistrés en tant que partenaires contractuels. En cas de correspondance, ils reçoivent une alerte silencieuse et peuvent voir, par exemple, si les billets ont déjà fait l'objet d'une enquête officielle dans un autre contexte (achats tests de stupéfiants, paiements de rançons, arnaques au petit-fils ou escroqueries liées à l'itinérance, explosions de distributeurs automatiques, etc.). Ils peuvent en outre obtenir des informations sur la date et le lieu d'impression des billets, savoir s'ils ont été mis en circulation ou épargnés récemment, connaître la < combinaison géographique > typique à laquelle leur mélange correspond, et bien plus encore », explique Gerrit Stehle.

Les informations ainsi obtenues permettent de répondre à des questions importantes en matière de tactique d'enquête, comme le montre Gerrit Stehle à l'aide d'exemples anonymisés tirés de la pratique.



Collectionneur inoffensif ou « mule » ?

À une frontière intra-européenne, les douanes trouvent 80 000 euros en espèces sur une personne. Cette dernière affirme avoir voulu acheter un objet de collection en Espagne et que le vendeur avait insisté pour être payé en espèces. Sur place, l'objet convoité s'est toutefois révélé douteux, raison pour laquelle l'achat a été annulé. L'argent apporté d'Allemagne lors du voyage a donc été ramené. « Dans un tel cas, les agents disposaient jusqu'à présent de peu de moyens de vérification », explique Gerrit Stehle. « Mais s'ils enregistrent les numéros des billets de banque, nous pouvons déterminer pour eux où ceux-ci ont été initialement produits. Cela permet ensuite de tirer des conclusions sur leur origine réelle. En effet, le pourcentage de billets en euros espagnols en circulation est naturellement beaucoup plus élevé en Espagne qu'en Allemagne. Si le pourcentage de billets espagnols parmi les billets transportés par cette personne était inférieur à 10 pour cent, cela renforcerait son affirmation. D'un autre côté, un pourcentage très élevé donnerait lieu à un soupçon initial justifié que cette personne pourrait être une < mule financière > ». »

Héritier ignare ou escroc sentimental peu scrupuleux ?

Autre exemple : Après plusieurs cas d'escroquerie sentimentale, les enquêteurs appréhendent un suspect. Sous une planche mal fixée dans sa cave, ils découvrent près de 55 000 euros en espèces répartis dans différentes enveloppes. Le suspect affirme ne pas être au courant de leur existence. Selon lui, c'est son père, décédé il y a huit ans et dont il a hérité la maison, qui a dû les cacher là. La police a des doutes et fait vérifier les numéros d'identification des billets. Il s'avère alors que les billets ont tous été en circulation au cours des dernières semaines et des derniers mois et ne peuvent donc certainement pas avoir été conservés dans une cave pendant des années. De plus, exactement 9 000 euros de l'argent suspect ont été retirés en plusieurs fois au cours des cinq derniers jours, au même distributeur automatique : celui de la banque d'une dame veuve de 55 ans. Comme le prouvent d'autres enquêtes, celle-ci fait également partie des victimes de l'escroc.

« Dans les cas d'arnaque au petit-fils, la vérification des numéros d'identification des billets trouvés sur les suspects peut également fournir des indices importants », révèle Gerrit Stehle. « En effet, c'est précisément dans ce type d'affaires que l'on trouve une quantité importante d'argent ancien, et les numéros d'identification nous permettent de déterminer où et quand les billets ont été produits. »

» Tandis que les armes peuvent être tracées grâce à l'enregistrement de leur numéro de série, les numéros d'identification des billets de banque ne sont jusqu'à présent pas enregistrés, ce qui ouvre la voie à des activités criminelles.



» Des appareils tels que le Glory GFS-220 (à droite sur la photo) permettent de compter, de trier et d'authentifier les billets de banque en un clin d'œil, mais aussi d'enregistrer leurs numéros d'identification.

Meurtrier et braqueur de banque ou individu chanceux ?

Troisième exemple : un vol est commis dans une commune rurale. Le malfaiteur, qui présente une cicatrice distinctive sur le front, dérobe environ 150 000 euros. L'affaire reste non résolue jusqu'à ce que, douze ans plus tard, des enquêteurs en civil, suivant une piste anonyme, identifient un suspect. Celui-ci présente une cicatrice caractéristique sur le front et les enquêteurs trouvent plus de 80 000 euros en espèces dans diverses cachettes de son appartement. L'homme clame son innocence et affirme avoir gagné cet argent au casino il y a deux ans. Il ne fait pas confiance aux banques, c'est pourquoi il le conserve chez lui. Pour le ministère public, l'affaire est claire, mais l'avocat commis d'office demande une analyse des numéros d'identification des billets de banque. Celle-ci prouve que les billets ont entre cinq et neuf ans, et n'existaient donc pas encore au moment du braquage de la banque. Résultat : acquittement !

Ces trois exemples montrent à quel point la traçabilité des billets de banque peut être précieuse pour les enquêtes et les poursuites pénales, et Gerrit Stehle pourrait en citer beaucoup d'autres. En effet, cette technologie a déjà été utilisée dans plus de 300 procédures pénales, notamment dans des affaires bancaires dites « hawala » liées au blanchiment d'argent ou au financement du terrorisme.

Une technologie également précieuse pour les détaillants et les services bancaires innovants

Outre les services de police et les autorités judiciaires, les entreprises qui manipulent régulièrement d'importantes sommes d'argent liquide peuvent également en bénéficier, et les banques peuvent offrir à leurs clients des services entièrement nouveaux.

« Les détaillants qui manipulent beaucoup d'argent liquide le comptent, le placent dans des conteneurs de transport et remplissent une pré-déclaration avant qu'un prestataire de services ne vienne récupérer l'argent. Si les entreprises enregistraient les numéros des billets lors du comptage, elles sauraient précisément lesquels leur appartiennent.

En cas de réclamation, par exemple pour trois < faux billets de 50 > dans le conteneur, elles pourraient prouver s'ils proviennent réellement d'elles ou s'ils ont été introduits ultérieurement par des tiers en échange de vrais billets de 50 », explique Gerrit Stehle.

Les banques pourraient quant à elles proposer à leurs clients, en cas de retraits d'espèces importants ou inhabituels, d'enregistrer les numéros d'identification des billets et de les sauvegarder sur une clé USB. « En cas d'extorsion, de fraude, de vol ou de toute autre perte, les billets pourraient être tracés », explique Gerrit Stehle. « Dès que les billets sont enregistrés par une société de transport de fonds, le système déclenche une alerte. Puisque le numéro de la « bombe financière » dans laquelle se trouvait l'argent est également connu, sa provenance est clairement identifiée. Les enquêteurs savent ainsi rapidement où rechercher d'autres traces des auteurs. Il en va de même lorsque les auteurs déposent l'argent quelque part. La < bombe d'encre numérique > explose alors également. »

Et bien sûr, il recommande vivement à toutes les banques d'enregistrer les numéros d'identification de tous les billets chargés dans les distributeurs automatiques : « La bombe d'encre numérique protège les billets de banque et permet un suivi rapide et efficace en cas d'explosion d'un distributeur automatique. »

Une technologie utilisable devant les tribunaux

Selon Gerrit Stehle, l'examen des procédures administratives nécessaire à l'admissibilité de la méthode devant les tribunaux s'est déroulé de manière aussi positive que les contrôles relatifs à la protection des données et des personnes. « Toutes les données sont stockées sur des serveurs certifiés, spécialement sécurisés et conformes aux normes d'audit en Allemagne, et peuvent être répliquées à 100 percento sur des infrastructures courantes telles que des serveurs fédéraux, des clouds souverains ou des centres de données locaux des autorités de sécurité », souligne-t-il. « Les autorités peuvent ainsi consulter de manière sécurisée les ensembles de données adaptés à leurs besoins en fonction des circonstances. » De plus, aucune donnée personnelle n'est collectée, car les transporteurs de fonds s'occupent généralement d'entreprises et non de personnes physiques.

Bientôt disponible en Suisse également ?

Outre Transparency International, certains parquets généraux et de nombreuses autorités judiciaires allemandes, des autorités de sécurité étrangères ont déjà pris connaissance de cette innovation allemande, notamment en Suisse, où des discussions sont en cours avec des acteurs importants, comme le révèle Gerrit Stehle.

Son entreprise développe actuellement, en coopération avec le spécialiste suisse OVD KINEGRAM AG, l'application « BANKNOTE SCANNER » [voir l'article dans la rubrique « Test et technologie »] qui permet de compter les billets de banque et d'enregistrer leurs numéros d'identification, même en déplacement. Rapide, simple et fiable.

Anche le banconote presentano delle impronte digitali: Sulle tracce dei biglietti incriminati

La Frankfurter Elephant & Castle IP GmbH ha sviluppato quello che tutte le forze dell'ordine attendevano con ansia dall'invenzione della banconota: un metodo per tracciare i singoli biglietti. Questo rivoluziona le possibilità di indagine e investigazione.



» Nei casi di truffa del falso nipote, i malfattori spesso rubano banconote molto vecchie (accumulate in casa). L'età di una banconota è rivelata dal suo numero identificativo. Questo consente di effettuare delle conclusioni.

A volte le sfide sono cristalline come un lago di montagna ma le soluzioni, pur essendo ovvie, risultano incredibilmente complesse e richiedono molto tempo nella pratica. È qui che le cose si complicano, come accaduto finora con il tracciamento pratico delle banconote incriminate o quantomeno sospette.

Queste ultime esistono in Svizzera da 200 anni, come sa chiunque abbia letto GIROFARO BLU 03-2025. E tutte le banconote sono contrassegnate con un numero di identificazione alfanumerico fin dalla prima serie. Detto numero, in combinazione al taglio e al tipo di valuta, rende ogni banconota unica. Inoltre, consente di trarre conclusioni inequivocabili sul momento e sul luogo di produzione (Paese e tipografia) e talvolta persino sul singolo foglio di stampa utilizzato per produrla. Se il numero di identificazione di una banconota segue anche una logica matematica, è possibile utilizzare un calcolo della cifra di controllo per verificarne l'autenticità.

L'impronta digitale di ogni biglietto

Per quanto ingegnoso possa essere il sistema consolidato dell'impronta digitale alfanumerica su ogni banconota, il suo utilizzo pratico per investigatori e forze dell'ordine è rimasto limitato, almeno finora. Mentre i numeri di identificazione vengono registrati e documentati durante la produzione e l'emissione iniziale delle valute moderne, una volta che le banconote entrano in circolazione, nessuno presta più attenzione ai loro numeri. Le banche non registrano quali banconote erogano a chi, a che ora ed in quale filiale durante i prelievi allo sportello. Analogamente, molte banconote finiscono negli sportelli bancomat senza che i loro numeri siano stati precedentemente registrati. Naturalmente, né i rivenditori né i ristoratori penserebbero mai di annotare i numeri di identificazione delle banconote che cambiano proprietario, in nessuna delle due direzioni. Per non parlare dei privati! Il «denaro registrato» noto nei romanzi polizieschi, ossia le banconote i cui numeri venivano registrati nonostante i criminali richiedessero «un milione in banconote di piccolo taglio non numerate», è pura finzione hollywoodiana.

Il contante come mezzo preferito dei criminali...

Ecco perché il denaro contante è stato il mezzo preferito dei criminali fin dalla sua invenzione, e sta cadendo sempre più in discredito. «La carta moneta è immensamente costosa, ed è la radice di tutti i mali», affermano i critici del denaro contante. Ma è davvero così?

La risposta di Gerrit Stehle, Managing Partner di Elephant & Castle IP GmbH, a questa domanda potrebbe sorprendervi. Egli si dice convinto dei meriti del sistema contante: «Le banconote sono un mezzo di pagamento che ha dimostrato la sua efficacia per secoli. Facili da maneggiare, fondamentalmente sicure e integrate in un'economia circolare eccellente e comprovata a livello internazionale.»

Dal suo punto di vista, l'unico aspetto negativo è che l'importanza cruciale del numero di identificazione è stata ignorata per troppo tempo, a causa della mancanza di tecnologie che ne consentissero un utilizzo efficiente. «La sfida è chiara: chiunque voglia porre fine alle attività criminali deve essere in grado di tracciare il percorso delle banconote. La soluzione esiste: il numero di identificazione, grazie al quale ogni banconota può essere identificata e tracciata.» Tuttavia, fino a poco tempo fa, nessuno aveva idea di quali tecnologie utilizzare per rendere questo processo il più semplice e veloce possibile», afferma Gerrit Stehle.

... finché Gerrit Stehle e il suo team non hanno avuto un'idea brillante

Quasi un decennio fa, lui e il suo team hanno affrontato questo problema e sviluppato un metodo brevettato che offre alle forze dell'ordine nuove possibilità rivoluzionarie. «Rendiamo il flusso di denaro nell'Eurozona visibile, utilizzabile e tracciabile nel rispetto dello stato di diritto», afferma Gerrit Stehle. «Utilizzando un software proprietario, un enorme database e in stretta collaborazione con vari partner attivi nel sistema di pagamento contante tradizionale, in particolare società di trasporto valori e Cash Center. La protezione dei dati e i diritti della personalità sono tutelati, l'anonimato del denaro contante non viene sostanzialmente compromesso e, naturalmente, distinguiamo tra flussi di denaro digitali e fisici. Inoltre, il sistema supporta le soluzioni software già in uso presso la polizia e le forze dell'ordine.»

Sembra allettante, ma quanto impegno richiede? «È gestibile», sottolinea Gerrit Stehle.



» Caso d'uso concreto: grazie alla registrazione automatica del numero identificativo, la logistica del contante diventa notevolmente più sicura.

Come funziona il tracciamento digitale dei contanti

Come prima fase, le società di trasporto valori hanno registrato i numeri di identificazione del maggior numero possibile di banconote, utilizzando moderni dispositivi di conteggio e verifica del denaro, come quelli già impiegati da anni da autorità federali, banche e spesso anche dai rivenditori (più grandi). «I dispositivi migliori non sono solo in grado di contare, ordinare e riconoscere l'autenticità di banconote di diverse valute tramite OCR (riconoscimento ottico dei caratteri), ma anche di registrare e memorizzare simultaneamente i loro numeri di identificazione, con una velocità di fino a 1'000 banconote al minuto», spiega Gerrit Stehle. «È fondamentale che non si verifichino errori durante la registrazione dei numeri e che eventuali problemi, come banconote sporche, siano chiaramente identificati», sottolinea. Per questo, lui e il suo team hanno testato innumerevoli dispositivi disponibili sul mercato, ciascuno con 10'000 banconote. «Chi desideri sapere quali hanno funzionato bene e quali no può contattarci e forniremo i risultati dei test», afferma Stehle.

Nella seconda fase, i numeri di identificazione registrati, simili alle impronte digitali, vengono inseriti in un database. «Se gli investigatori o le forze dell'ordine cercano banconote specifiche, possono, una volta registratisi come partner contrattuali, cercarle nel database della nostra azienda. In caso di corrispondenza, ricevono un avviso silenzioso e possono verificare, ad esempio, se le banconote siano state precedentemente di interesse per le autorità in un altro contesto (ad esempio, acquisti per test antidroga, pagamenti di riscatti, la truffa del falso nipote o le truffe sentimentali, esplosione di sportelli bancomat, ecc.). Possono anche ottenere informazioni su quando e dove siano state stampate le banconote, se siano state in circolazione di recente o se siano state accumulate, a quale «Paese» corrisponde la loro composizione e molto altro ancora», spiega Gerrit Stehle.

Le informazioni ottenute in questo modo possono rispondere a importanti domande tattiche investigative, come dimostra Gerrit Stehle utilizzando esempi pratici resi anonimi.

Un collezionista innocuo o un «Cash Mule»?

I funzionari doganali hanno trovato 80'000 euro in contanti addosso a una persona a un confine intraeuropeo. Questa ha affermato di voler acquistare un pezzo da collezione in Spagna e che il venditore aveva insistito per un pagamento in contanti. Tuttavia, una volta sul posto, l'oggetto del desiderio si era rivelato sospetto, motivo per cui l'acquisto era fallito e il denaro, che aveva già portato con sé dalla Germania, era stato riportato indietro. «In casi simili, i funzionari avevano finora pochi mezzi di verifica», afferma Stehle. «Ma se registrano i numeri di serie delle banconote, possiamo scoprire per loro dove queste siano state originariamente prodotte. Ciò permette quindi di trarre conclusioni sulla loro effettiva origine. Perché la percentuale di banconote spagnole in euro in circolazione è naturalmente molto più alta in Spagna che in Germania. Se il valore fosse, ad esempio, nell'intervallo percentuale a una sola cifra, ciò rafforzerebbe quanto affermato dalla persona. D'altra parte, una percentuale molto elevata solleverebbe un ragionevole sospetto sul fatto che la persona in questione possa essere un «Money Mule».»

Erede inconsapevole o truffatore sentimentale spietato?

Un altro esempio: dopo diverse truffe sentimentali, gli inquirenti fermano un sospettato. Sotto un'asse smossa del pavimento nella sua cantina, trovano quasi 55'000 euro in contanti in diverse buste. Il sospettato afferma di non saperne nulla. Sostiene che suo padre, morto otto anni prima e da cui ha ereditato la casa, deve averli nascosti lì. La polizia nutre dei dubbi e fa controllare i numeri di serie delle banconote. A quanto pare: tutte le banconote erano state in circolazione nelle ultime settimane e mesi, quindi non potevano essere rimaste in cantina per anni. Inoltre, esattamente 9'000 euro del denaro sospetto erano stati prelevati in più fasi nei cinque giorni precedenti dallo stesso bancomat della banca di una vedova di 55 anni. Da ulteriori indagini si scopre poi che anche lei era tra le vittime del truffatore.

«Anche nei casi di truffa del falso nipote, controllare i numeri di identificazione delle banconote trovate addosso ai sospettati può fornire indizi importanti», rivela Gerrit Stehle. «Questo perché in questi casi compare una quantità significativa di denaro vecchio, e possiamo usare i numeri di identificazione per dimostrare dove e quando sono state prodotte le banconote.»

» Il sistema E&C consente di rintracciare le banconote rubate durante le esplosioni di sportelli bancomat (qui in Germania, Viersen, 2021), a condizione che i numeri delle banconote siano stati precedentemente registrati nello sportello bancomat.



FÜR ALLE, DIE DIE SCHWEIZ AM LAUFEN HALTEN!

Die Schweizer Fachmesse für den
öffentlichen Sektor auf dem BERNEXPO-Areal.



Jetzt
entdecken

**SUISSE
PUBLIC**

**16. –
19.06.
2026**



» Se le banche offrissero la registrazione dei numeri di identificazione come servizio al prelievo di contanti, le banconote potrebbero essere rintracciate in caso di truffa, come le truffe sentimentali.

Assassino e rapinatore di banche o solo fortunato?

Un terzo caso: avviene una rapina in una comunità rurale. L'autore, con una caratteristica cicatrice sulla fronte, si porta via circa 150'000 euro. Il caso rimane irrisolto finché, dodici anni dopo, degli inquirenti in borghese, agendo su una soffiata anonima, si concentrano su un sospettato. Quest'uomo ha una vistosa cicatrice sulla fronte e, nel suo appartamento, gli inquirenti trovano più di 80'000 euro in contanti nascosti in vari posti. L'uomo si dichiara innocente, sostenendo di aver vinto il denaro in un casinò due anni prima. Non si fida delle banche, motivo per cui lo conserva in casa. Per il Ministero pubblico, il caso è chiaro, ma il difensore d'ufficio ordina un'analisi dei numeri di serie delle banconote. Da questa emerge che le banconote hanno un'età compresa tra i cinque e i nove anni, il che significa che non esistevano nemmeno al momento della rapina in banca. Risultato: l'assoluzione!

Tre esempi che dimostrano quanto la tracciabilità delle banconote possa essere preziosa per indagini e procedimenti penali. E Gerrit Stehle potrebbe citarne molti altri. Infatti, questa tecnologia è già stata utilizzata in oltre 300 procedimenti penali, inclusi i cosiddetti casi bancari «hawala», utilizzati per riciclaggio di denaro o finanziamento del terrorismo.

Preziosa anche per i rivenditori e per i servizi di smart banking

Oltre a indagini e procedimenti penali, anche le aziende che gestiscono regolarmente grandi quantità di denaro contante possono trarne vantaggio, mentre le banche potrebbero offrire ai propri clienti servizi completamente nuovi.

«I rivenditori che gestiscono grandi quantità di denaro contante lo contano, lo imballano in contenitori per il trasporto, inviano una notifica preventiva e un fornitore di servizi ritira il denaro. Se le aziende registrassero i numeri di serie delle banconote durante il conteggio, saprebbero esatta-

mente quali banconote appartengono a loro.» «In caso di reclami, ad esempio riguardanti tre presunte «banconote false da 50 euro» nel contenitore, potrebbero dimostrare se queste banconote appartenessero effettivamente a loro o se siano state successivamente mischiate da terzi in cambio di banconote da 50 euro autentiche», sottolinea Gerrit Stehle.

Le banche, a loro volta, potrebbero offrire ai propri clienti la possibilità di registrare i numeri di identificazione delle banconote e salvarli su una chiavetta USB quando effettuano prelievi di contanti di importi elevati o inusuali. «In caso di estorsione, truffa, furto o altra perdita, le banconote potrebbero essere rintracciate», afferma Gerrit Stehle. «Non appena le banconote vengono registrate presso una società di trasporto valori, il sistema attiva un allarme. Poiché è noto anche il numero della cassetta in cui erano contenute, ne è chiara la provenienza. Ciò consentirebbe agli investigatori di determinare rapidamente dove cercare ulteriori indizi. Lo stesso accade se gli autori del reato depositano il denaro da qualche parte. Anche in questo caso si attiva «il sistema digitale di macchiatura».

Naturalmente, egli consiglia vivamente a tutte le banche di registrare i numeri di identificazione di tutte le banconote caricate negli sportelli bancomat: «Il sistema digitale di macchiatura protegge le banconote e consente un tracciamento rapido ed efficace in caso di esplosione di sportelli bancomat.»

La tecnologia è ammissibile in tribunale

Secondo Gerrit Stehle, la revisione delle procedure ufficiali necessarie per l'ammissibilità del metodo in tribunale ha avuto successo tanto quanto le verifiche sulla protezione dei dati e della personalità. «Tutti i dati sono archiviati su server certificati, appositamente protetti e a prova di audit in Germania e possono essere opzionalmente replicati al 100 per cento su infrastrutture comuni come server federali, cloud sovrani o data center locali delle autorità di sicurezza», sottolinea. «Ciò consente alle autorità di accedere in modo sicuro a set di dati personalizzati in base alle loro esigenze specifiche.» Inoltre, non vengono raccolti dati personali, poiché le società di trasporto valori servono generalmente aziende e non privati.

Presto disponibile anche in Svizzera?

Oltre a Transparency International, alcuni Ministeri pubblici generali e numerose forze dell'ordine tedesche, anche delle autorità di sicurezza straniere hanno già mostrato interesse per l'innovazione tedesca, comprese quelle svizzere, dove sono in corso discussioni con i principali stakeholder, come rivela Gerrit Stehle.

Inoltre, la sua azienda sta attualmente sviluppando l'app «BANKNOTE SCANNER» (vedi l'articolo nella sezione «Test e Tecnica» di questo numero) in collaborazione con l'azienda svizzera specializzata OVD KINEGRAM AG. Questa app consente di contare le banconote e di registrarne i numeri di identificazione in modo rapido, semplice e affidabile, anche su dispositivi mobili.

Lösungen für Behörden zur Kontrolle von Tachographen und der Arbeitszeit von Fahrern



**Besuchen Sie uns
an der SPIK 2026
in Bern**

- ✓ Software
- ✓ DSRC
- ✓ Downloading devices
- ✓ Training

Kontakt

Jörg Harmening

Enforcement Authority Services and Export Sales Manager D-A-CH
jorg.harmening@eurowag.com

+49 15 750 761 314 / +420 734 260 766

TachoScan Control

Präzise und effiziente Kontrolle von Lenk- und Ruhezeiten

TachoScan Control ist eine leistungsfähige Softwarelösung zur Auswertung digitaler Tachographendaten und Fahrerkarten. Die Anwendung richtet sich insbesondere an Kontrollbehörden, Polizei- und Aufsichtsorgane, die eine rechtskonforme, effiziente und strukturierte Analyse von Lenk- und Ruhezeiten benötigen.

Die Software ermöglicht das Auslesen und die detaillierte Auswertung von Daten aus digitalen Tachographen. In der Schweiz erfolgt die Kontrolle insbesondere auf Grundlage der ARV (Arbeits- und Ruhezeitverordnung) sowie der entsprechenden nationalen Vorschriften. Verstöße gegen Lenk-, Ruhe- und Arbeitszeiten werden automatisiert erkannt und transparent dargestellt. Dadurch werden Kontrollprozesse deutlich beschleunigt und revisionssicher dokumentiert.

Ein zentrales Merkmal von TachoScan Control ist die übersichtliche grafische Darstellung der Fahrtstätigkeiten. Tages-, Wochen- und Mehrwochenanalysen ermöglichen eine schnelle Identifikation von Unregelmässigkeiten. Darüber hinaus können Unternehmensdaten, Fahrzeugbewegungen, Geschwindigkeitsverläufe sowie mögliche Manipulationshinweise systematisch geprüft werden. Umfangreiche Berichtsfunktionen sorgen für eine nachvollziehbare Dokumentation im Rah-

men von Verwaltungs- oder Strafverfahren.

TachoScan Control wird unter anderem von renommierten Behörden wie der Stadtpolizei Zürich sowie der Kantonspolizei Bern eingesetzt. Diese Institutionen vertrauen auf die zuverlässige Analysefunktion, die hohe Rechtssicherheit und die kontinuierliche Weiterentwicklung der Software.

Die Lösung wird regelmässig auf Fachveranstaltungen präsentiert, darunter auch auf dem SPIK in Bern, der als zentrale Plattform für den Austausch zwischen Behörden, Experten und Anbietern im Bereich Verkehrskontrolle gilt.

Für weitere Informationen und als Ansprechpartner in der DACH-Region steht zur Verfügung:

Jörg Harmening
Enforcement Authority Services
and Export Sales Manager DACH
 E-Mail: jorg.harmening@eurowag.com
 Tel.: +420 734 260 766

TachoScan Control leistet damit einen wesentlichen Beitrag zur Verkehrssicherheit und zur konsequenten Durchsetzung der Sozialvorschriften im Strassenverkehr – unterstützt durch fachliche Expertise und persönliche Betreuung im deutschsprachigen Raum.





5 JAHRE
HERSTELLER-
GARANTIE

Herstellergarantie endet nach 5 Jahren oder einer maximalen Gesamtleistung von 200'000 km.
Weitere Informationen und Garantiebedingungen unter volkswagen-nutzfahrzeuge.ch

Bereit für jeden Einsatz. Der neue Caravelle

Gerade wenn jede Sekunde zählt, überzeugt der neue VW Caravelle mit Funktionalität, Zuverlässigkeit und Robustheit. Und dank dem spezialisierten Behördenausbau wird aus ihm ein hochfunktionales Einsatzmittel. Denn im Einsatzdienst gibt es keinen Raum für Kompromisse. Mit ihm und seiner modernen Technik und seinen hochwertigen Materialien meistern Sie auch die Ansprüche intensiver Arbeitsalltage.
VW Nutzfahrzeuge. Die beste Investition.



Nutzfahrzeuge



» Am 16. und 17. März 2026 findet in Bern die 18. Auflage des Schweizer Polizei Informatik Kongresses SPIK statt – dieses Jahr erstmals in der neuen Festhalle in Bern.

SPIK 2026:

Umzug in die Festhalle in Bern

Die 18. Austragung des Schweizer Polizei Informatik Kongresses SPIK erstreckt sich wie schon im Vorjahr auf zwei Tage – und findet erstmalig in der neuen BERNEXPO-Festhalle statt.

Eineinhalb Tage SPIK 2026

Seit zwei Jahren befindet sich der Schweizer Polizei Informatik Kongress (SPIK) auf Höhenflug. Organisiert vom Verein Swiss Police ICT in Kooperation mit der Berner Agentur ZONE B markierten die Austragungen in den Jahren 2024 und 2025 jeweils Rekordmarken. In beiden Jahren wuchs die Zahl der Aussteller, es gab mehr Fachreferate und die Gästeschar wurde grösser. 2025 strömten total mehr als 1'000 Angehörige der Schweizer Blaulichtorganisationen sowie zahlreicher Systemanbieter nach Bern. Zahlreiche von ihnen blieben sogar über Nacht in der Bundesstadt – denn 2025 fand am Vortag des eigentlichen SPIK erstmals der «MSK-Halbttag» statt, eine Tagung mit Fokus auf die geplante «Mobile Sichere Breitbandkommunikation MSK», die das Polycom-System dereinst ablösen soll.

Da das Konzept des SPIK von den Zielgruppen sehr gut aufgenommen wird und 2025 alles «wie am Schnürchen» funktionierte, bleiben die Rahmenbedingungen 2026 nahezu unverändert. Tag 1, am 16. März 2026, ist dem Aufbau (Vormittag) sowie dem MSK-Halbttag gewidmet. Dieser startet um 13.15 Uhr mit der Begrüssung und der Eröffnungsrede, gefolgt von einer Keynote. Ab 15 Uhr dann stehen – in zwei Parallelsessions – gesamthaft vier Referate rund um das Thema «Mobile Sichere Breitbandkommunikation» auf dem Programm. Diese werden von den Unternehmen Swissphone, Swisscom, Huawei und Airbus bestritten und dauern jeweils 45 Minuten. Dazwischen liegt eine 15-minütigen Pause. Zum Abschluss des MSK-Halbtages, ab 17 Uhr, lädt die Organisation viele zum Apéro und Networking ein.

Am zweiten Tag, dem 17. März 2026, findet die traditionelle Standmesse statt – wobei gut die Hälfte der Stände auch schon während des MSK-Halbtags geöffnet sein werden. Tag 2 startet um 8.45 Uhr (Einlass ab 7.30 Uhr) und dauert bis 18 Uhr. Parallel haben die Gäste die Möglichkeit, ihr Fachwissen bei 20 Referaten auf den neuesten Stand zu bringen. Die Vorträge finden in vier Sälen statt, dauern je 30 Minuten – und widmen sich wie jedes Jahr sehr vielfältigen Themenkreisen.

Wieder mit «NEDIK»-Fachtagung

Ein dritter wesentlicher Bestandteil des SPIK ist auch dieses Jahr das «Netzwerk digitale Ermittlungsunterstützung Internetkriminalität NEDIK». Zum dritten Mal gewähren Spezialisten des Netzwerks vertiefte Einblicke in ihre Arbeit, zu Fällen und Kooperationen. Die Teilnahme an jedem der vier NEDIK-Referate ist wie immer exklusiv den Kräften der Polizeikörpers sowie Angehörigen von Staatsanwaltschaften vorbehalten.

Mehr als vier Dutzend Aussteller

Die Vielfalt der an der Tischmesse des SPIK teilnehmenden Unternehmen bewegt sich auf vergleichbar hohem Niveau wie im Vorjahr. Bis Januar 2026 waren gemäss Auskunft der Organisation 52 Sponsoren angemeldet. Eintönigkeit ist entsprechend keineswegs zu erwarten. Zwar sind nicht wenige Sponsoren wie beispielsweise Hexagon, Swisscom, Unisys, Abraxas, sureVive oder Airbus – um nur einige zu nennen – seit vielen Jahren treue Unterstützer respektive Teilnehmer am SPIK. Doch wie jedes Jahr sind auch bei der 18. Auflage des SPIK wieder zahlreiche neue Unternehmen am Start.

Breites Spektrum an Themen geplant

Ein Blick auf die Themenliste der 2026 beim SPIK anstehenden Fachvorträge offenbart: Die Möglichkeiten, Chancen und Risiken von KI-Lösungen im Blaulichtsektor stehen einmal mehr im Fokus diverser Referate. Beispielsweise fokussiert die rola Security Solutions GmbH auf das Thema «KI-gestützte Bild- und Videoanalyse als Ermittlungswerkzeug der Zukunft». Die IABG GmbH gibt Einblicke, wie KI-Lösungen die Aufgaben von und die Tätigkeiten in Leitstellen beeinflusst und worauf bei entsprechenden Planungen zu achten ist. Und die PricewaterhouseCoopers AG beleuchtet die Transformation polizeilicher Kernprozesse durch rechtssichere KI-Lösungen.

Aber auch die Themenkreise Kommunikation und (Cyber-) Sicherheit kommen nicht zu kurz. Die smaro GmbH zeigt auf, wie die moderne und sichere Kommunikation auf Einsatzleitfahrzeugen der Zukunft aussieht (Bonding-Kommunikation) und Motorola Solutions beleuchtet, wie eine nahtlose Einsatzkommunikation unter Einbezug von Bodycams und Funk möglich wird.

Im Bereich Cybersicherheit widmet sich die Wavestone Consulting Switzerland AG dem Thema «Digitalisierung der Strafjustiz: Cyberresilienz als gemeinsame Aufgabe von Polizei, Justiz und IT», während die ELCA Informatik AG Interessierten näherbringt, wie Cybersicherheit bei Grossveranstaltungen gewährleistet werden kann.

Spezialisten der Abraxas Informatik AG referieren über «IAM PTI – Identity und Access Management als Schlüssel zur sicheren Zusammenarbeit von Polizeikörpers» – und für Forensiker empfehlen wir den Fachvortrag «Das forensische Labor in der Hosentasche: Wie iPhones die Spurensicherung und Einvernahme revolutionieren», präsentiert von der PIC Systems AG.



» An den Hubs der Sponsoren erhalten die Gäste Informationen aus erster Hand – und auch das Networking und der Austausch mit Fach- und Berufskollegen kommen nicht zu kurz.

«Fakten & Zahlen»

SPIK 2026

Türöffnung zum «MSK-Halbttag» am Montag, 16. März 2026, ist um 12.30 Uhr. Das Programm startet um 13.15 Uhr. Geplant sind neben einer Eröffnungsrede und einer Keynote vier Referate von je 45 Minuten Dauer (zwei Parallelsessions in zwei Räumen). Ab 17 Uhr findet ein Apéro statt. Der Anlass endet um 18 Uhr.

Türöffnung zum SPIK-Haupttag am Dienstag, 17. März 2026, ist um 7.30 Uhr. Das Tagesprogramm startet um 8.45 Uhr mit der Begrüssungsrede, gefolgt von einem Plenumsreferat zum Thema «Drohnen». Ab 10 Uhr stehen die 20 Fachreferate und vier NEDIK-Beiträge auf der Tagesordnung. Diese finden in vier Räumlichkeiten statt. Mittagspause ist von 12 bis 13 Uhr. Um 13 Uhr findet das Mittagsplenum statt, die zweite Welle der Vorträge beginnt um 14 Uhr. Ab 16 Uhr besteht beim Apéro nochmals die Möglichkeit zum Networking. Offizielles Ende des SPIK 2026 ist um 18 Uhr.

Weiterführende **Informationen** inklusive Details zu Programm, Location und Anreise finden Interessierte auf www.swisspoliceict.ch.

Das **Ticketing** läuft über: www.eventfrog.ch

Sehr konkret wird es wie immer bei jenen Fachbeiträgen, die sich laufenden oder kürzlich abgeschlossenen Beschaffungsprojekten widmen. Beispiele beim SPIK 2026 sind die Einführung des Mico-Kommunikationssystems bei der Kantonspolizei Tessin (Projekt NOTIS; Supercomputing Systems AG) sowie die Modernisierung der Sanitätsnotrufzentrale der Kantonalen Walliser Rettungsorganisation KWRO (HxGN Schweiz AG).

Tickets und Teilnahme

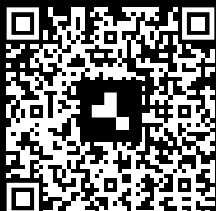
Alle, die den SPIK 2026 und/oder den «MSK-Halbttag» besuchen wollen, benötigen pro Teilnahme-Tag jeweils ein entsprechend gesondertes Ticket (siehe Box). Diese sind wie immer für Vertreter der Wirtschaft und Private kostenpflichtig, während Angehörige von Behörden, Verwaltung, Blaulichtorganisationen etc. von freiem Eintritt profitieren.

sureVIVE

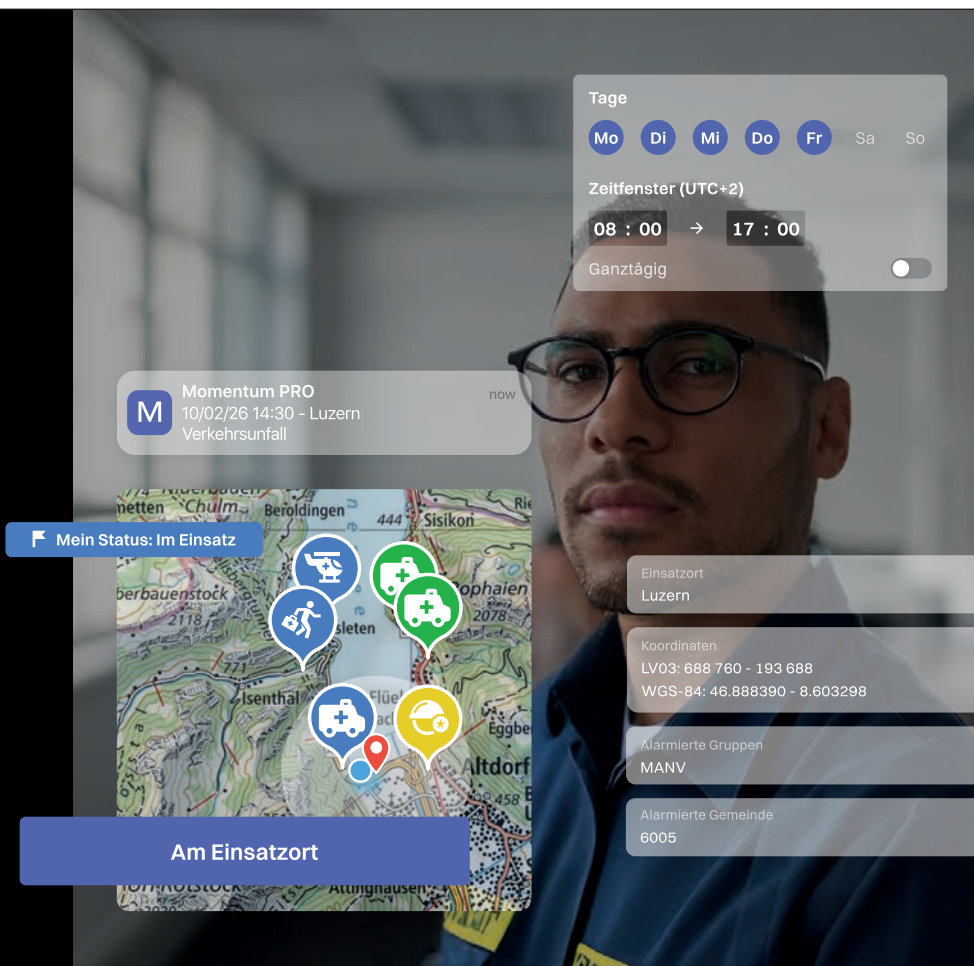
Alles unter Kontrolle.

Alles auf einen Blick.

Scanne den QR-Code, um zu erfahren, wie wir dich unterstützen können.



• • • swiss
• emergency
— • • data
• • • • hub





» Les 16 et 17 mars 2026, la 18^e édition du Congrès suisse sur l'informatique policière (SPIK) se tiendra à Berne, pour la première fois cette année dans la nouvelle Festhalle de Berne.

SPIK 2026: Déménagement dans la Festhalle à Berne

La 18^e édition du Congrès suisse sur l'informatique policière (SPIK) se déroule, comme l'année dernière, sur deux jours et a lieu pour la première fois dans la nouvelle salle BERNEXPO.

Un jour et demi pour le SPIK 2026

Depuis deux ans, le Congrès suisse sur l'informatique policière (SPIK) connaît un succès croissant. Organisé par l'association Swiss Police ICT en collaboration avec l'agence bernoise ZONE B, les éditions 2024 et 2025 ont chacune battu des records. Ces deux éditions ont vu le nombre d'exposants et de visiteurs augmenter et le nombre de conférences spécialisées se multiplier. En 2025, plus de 1 000 membres des organisations d'urgence suisses et de nombreux fournisseurs de systèmes se sont rendus à Berne. Beaucoup d'entre eux ont même passé la nuit dans la capitale fédérale, car en 2025, la veille du SPIK, s'est tenue pour la première fois la « demi-journée MSK », une conférence consacrée au projet « Communication mobile sécurisée à large bande MSK », qui doit un jour remplacer le système Polycorn.

Le concept du SPIK ayant été très bien accueilli par les groupes cibles et tout ayant fonctionné « comme sur des roulettes » en 2025, les conditions générales restent pratiquement inchangées en 2026. Le premier jour, le 16 mars 2026, est consacré à l'installation (le matin) et à la demi-journée MSK. Celle-ci débute à 13h15 par l'accueil des visiteurs et le discours d'ouverture, suivi d'une allocution. À partir de 15h, quatre conférences sur le thème « Communication mobile sécurisée à large bande » sont organisées en deux sessions parallèles. Ces exposés sont présentés par les entreprises Swissphone, Swisscom, Huawei et Airbus et durent chacun 45 minutes. Une pause de 15 minutes est prévue entre les exposés. À la fin de la demi-journée MSK, à partir de 17h, l'organisation invite les participants à un cocktail de réseautage.

Le deuxième jour, le 17 mars 2026, a lieu le salon traditionnel, dont plus de la moitié des stands seront déjà ouverts pendant la demi-journée MSK. Le deuxième jour débute à 8h45 (ouverture des portes à 7h30) et se termine à 18h. En parallèle, les visiteurs ont la possibilité d'actualiser leurs connaissances spécialisées grâce à 20 conférences. Les conférences se déroulent dans quatre salles, durent chacune 30 minutes et portent, comme chaque année, sur des thèmes très variés.

Le colloque « NEDIK » de retour

Cette année encore, le « Réseau de soutien aux enquêtes dans la lutte contre la criminalité informatique NEDIK » constitue un troisième élément essentiel du SPIK. Pour la troisième fois, les spécialistes du réseau offrent un aperçu approfondi de leur travail, des affaires traitées et des coopérations. Comme toujours, la participation à chacune des quatre conférences du NEDIK est réservée exclusivement aux membres des corps de police et aux représentants des ministères publics.

Plus de quatre douzaines d'exposants

La diversité des entreprises participant au SPIK est comparable à celle de l'année dernière. Selon les informations fournies par l'organisation, 52 sponsors étaient inscrits en janvier 2026. La monotonie ne sera donc pas non plus au rendez-vous de cette édition. Certes, bon nombre de sponsors, tels que Hexagon, Swisscom, Unisys, Abraxas, sureVive ou Airbus, pour n'en citer que quelques-uns, sont des soutiens ou des participants fidèles du SPIK depuis de nombreuses années. Mais comme chaque année, de nombreuses nouvelles entreprises seront présentes à la 18^e édition du SPIK.

Large éventail de thèmes couverts

Un coup d'œil à la liste des thèmes des conférences spécialisées prévues pour le SPIK 2026 révèle une chose : Les possibilités, les opportunités et les risques des solutions d'IA dans le secteur des services d'urgence sont une fois de plus au centre de diverses conférences. Par exemple, rola Security Solutions GmbH se concentre sur le thème « L'analyse d'images et de vidéos assistée par l'IA comme outil d'enquête du futur ». L'entreprise IABG GmbH donne un aperçu de la manière dont les solutions d'IA influencent les tâches et les activités des centres de contrôle et des points à prendre en compte lors de la planification. PricewaterhouseCoopers AG met en lumière la transformation des processus policiers fondamentaux grâce à des solutions d'IA juridiquement sûres.

Les thèmes de la communication et de la (cyber) sécurité ne sont pas non plus oubliés. L'entreprise smaro GmbH montre à quoi ressemblera la communication moderne et sécurisée dans les véhicules de commandement du futur (communication bonding), tandis que Motorola Solutions met en lumière la manière dont une communication opérationnelle fluide est possible grâce à l'utilisation de bodycams et de radios.

Dans le domaine de la cybersécurité, Wavestone Consulting Switzerland AG aborde le thème « Numérisation de la justice pénale : la cyberrésilience comme mission commune de la police, de la justice et de l'informatique », tandis qu'ELCA Informatik AG explique aux personnes intéressées comment garantir la cybersécurité lors de grands événements.

Les spécialistes d'Abraxas Informatik AG présentent un exposé sur « IAM PTI - La gestion des identités et des accès comme clé d'une collaboration sécurisée entre les corps de police », et pour les experts en criminalistique, nous recom-



» Les visiteurs reçoivent des informations de première main aux stands des sponsors et pourront également profiter des occasions de réseautage et d'échange avec des collègues spécialisés et professionnels.

« Faits et chiffres » SPIK 2026



L'ouverture des portes pour la « **demi-journée MSK** » le **lundi 16 mars 2026** est prévue à partir de 12h30. Le programme débute à 13h15. Outre un discours d'ouverture et une allocution, quatre conférences de 45 minutes chacune sont prévues (deux sessions parallèles dans deux salles). Un cocktail est servi à partir de 17h. L'événement se termine à 18h.

L'ouverture des portes pour la journée principale du SPIK, le **mardi 17 mars 2026**, est prévue à 7h30. Le programme de la journée débute à 8h45 par le discours de bienvenue, suivi d'une présentation en plénière sur le thème des drones. À partir de 10h, les 20 conférences techniques et les quatre exposés du NEDIK sont à l'ordre du jour. Ces événements se déroulent dans quatre salles. La pause déjeuner est prévue de 12h à 13h. À 13h a lieu la séance plénière de midi, et la deuxième série de conférences commence à 14h. À partir de 16h, le cocktail offre une nouvelle occasion de réseautage. La clôture officielle du SPIK 2026 est prévue à 18h.

Pour plus d'informations, notamment sur le programme, le lieu et l'accès, rendez-vous sur www.swisspoliceict.ch.

La **billetterie** est disponible à l'adresse suivante : www.eventfrog.ch

mandons la conférence spécialisée « Le laboratoire médico-légal dans votre poche : comment les iPhone révolutionnent la collecte de preuves et les interrogatoires », présentée par l'entreprise PIC Systems AG.

Comme toujours, les exposés spécialisés consacrés aux projets d'acquisition en cours ou récemment achevés sont très concrets. Au SPIK 2026, on peut citer par exemple l'introduction du système de communication Mico par la police cantonale tessinoise (projet NOTIS ; Supercomputing Systems AG) et la modernisation de la centrale d'appel d'urgence sanitaire de l'organisation cantonale valaisanne de secours KWRO (HxGN Schweiz AG).

Billets et participation

Toute personne souhaitant assister au SPIK 2026 et/ou à la « demi-journée MSK » doit se procurer un billet distinct pour chaque jour de participation (voir encadré). Comme toujours, ces billets sont payants pour les représentants du monde économique et les particuliers, tandis que les membres des autorités, de l'administration, des organisations d'urgence, etc. bénéficient d'une entrée gratuite.

Ergonomische Arbeitsplätze für Einsatzzentralen

Besuchen Sie uns an der

spik
SWISS POLICE ICT

erichkeller
INTERIORS
COMMUNICATION DESKS
TALKY OFFICE
CLIMATE SYSTEMS



» Il 16 e il 17 marzo 2026 si terrà a Berna la 18ª edizione del Congresso di informatica della Polizia svizzera (SPIK), questa volta nella nuova sala feste della capitale.

SPIK 2026:

Trasferimento alla sala feste di Berna

La 18ª edizione del Congresso di informatica della Polizia svizzera (SPIK) si estende (come già lo scorso anno) a due giornate e si terrà per la prima volta nella nuova sala feste BERNEXPO.

Una giornata e mezza allo SPIK 2026

Da due anni, il Congresso di informatica della Polizia svizzera (SPIK) vive un'impegnata. Organizzato dall'associazione Swiss Police ICT, in cooperazione con l'Agenzia di Berna ZONA B, le edizioni del 2024 e del 2025 hanno raggiunto nuovi record. In entrambi gli anni, il numero di espositori è cresciuto, si sono tenute più presentazioni e anche il pubblico ospite è aumentato. Nel 2025 sono accorsi a Berna oltre 1'000 membri delle organizzazioni a girofaro blu e svariati fornitori di sistemi. Molti di loro hanno anche pernottato nella capitale perché nel 2025, il giorno prima dello SPIK vero e proprio si è tenuta per la prima volta la «mezza giornata CMS», un convegno incentrato sulla pianificata «comunicazione mobile a banda larga sicura CMS», che doveva sostituire il sistema Polycom di allora.

Dato che il concetto dello SPIK è ben accolto dai gruppi di destinazione e nel 2025 tutto ha funzionato alla perfezione, le condizioni per il 2026 rimangono pressoché invariate. Il giorno 1, il 16 marzo 2025, sarà dedicato all'allestimento (mattinata) e alla mezza giornata CMS. Questa avrà inizio alle ore 13.15, con il benvenuto e il discorso di apertura, seguita da un Keynote. A partire dalle ore 15.00, sono in programma (in sessioni parallele) quattro presentazioni sul tema «comunicazione mobile a banda larga sicura». Queste saranno tenute dalle società Swissphone, Swisscom, Huawei e Airbus e dureranno 45 minuti ciascuna, oltre ad una pausa di 15 minuti. Per concludere la mezza giornata CMS, a partire dalle ore 17.00, l'organizzazione invita ad un aperitivo di networking.

Il secondo giorno, il 17 marzo 2026, avrà luogo la tradizionale fiera con stand, sebbene una buona metà di questi sarà aperta già durante la mezza giornata CMS. Il giorno 2 inizierà alle ore 08.45 (ingresso dalle 07.30) e si chiuderà alle ore 18.00. In parallelo, gli ospiti potranno aggiornare le loro conoscenze partecipando alle 20 presentazioni in programma. Gli interventi, della durata di 30 minuti ciascuno, si terranno in quattro sale e avranno come oggetto temi molto diversificati.

Ancora una volta con convegno specialistico «NEDIK»

Una terza componente essenziale dello SPIK sarà anche quest'anno la «Rete di sostegno alle indagini nella lotta contro la criminalità digitale NEDIK». Per la terza volta, gli specialisti della rete garantiscono approfondimenti sul loro lavoro, su casi e cooperazioni. La partecipazione alle quattro presentazioni NEDIK è come sempre riservata esclusivamente alle forze dei corpi di polizia e ai membri dei Ministeri pubblici.

Oltre quattro dozzine di espositori

La varietà di imprese partecipanti alla fiera dello SPIK è paragonabile all'alto livello raggiunto già lo scorso anno. A gennaio 2026, a detta dell'organizzazione, si erano iscritti 52 sponsor. Il rischio di incappare in un evento monotono è pertanto scampato. Non solo sponsor della portata di Hexagon, Swisscom, Unisys, Abraxas, sureVive o Airbus (solo per citarne alcuni) supportano da molti anni o partecipano allo SPIK ma, come ogni anno, anche la 18ª edizione di questo evento saluterà il coinvolgimento di svariate nuove imprese.

Ampia gamma di temi in programma

Uno sguardo all'elenco dei temi trattati alle presentazioni in programma per lo SPIK 2026 rivela che molte relazioni si focalizzeranno sulle possibilità, sulle opportunità e sui rischi delle soluzioni IA nel settore a girofaro blu. Ad esempio, la rola Security Solutions GmbH si focalizza sul tema dell'«analisi di immagini e video tramite supporto IA come strumento di indagine del futuro». La IABG GmbH approfondisce come le soluzioni IA influenzino i compiti e le attività nei centri di controllo e a cosa bisogna fare attenzione nelle relative progettazioni. La PricewaterhouseCoopers AG fa luce sulla trasformazione dei processi centrali di polizia grazie a soluzioni IA conformi alla legge.

Ma anche i temi della comunicazione e della (ciber)sicurezza ricevono ampia attenzione. La smaro GmbH mostra come la comunicazione moderna e sicura vede i veicoli di controllo di emergenza del futuro (comunicazione Bonding) e Motorola Solutions illustra come sia possibile una comunicazione operativa senza interruzioni, comprese bodycam e sistemi radio.

Nel campo della ciber sicurezza, la Wavestone Consulting Switzerland AG si dedica al tema della «digitalizzazione della giustizia penale: cyber resilienza come compito comune tra polizia, giustizia e informatica», mentre la ELCA Informatik AG informa gli interessati su come la ciber sicurezza possa essere garantita in occasione di grandi eventi.

Gli specialisti di Abraxas Informatik AG riferiscono di «IAM PTI – Identity e Access Management come chiave per la collaborazione sicura dei corpi di polizia», mentre agli scienziati forensi suggeriamo la presentazione «Il laboratorio forense in tasca: come gli iPhones rivoluzionano la raccolta delle tracce e gli interrogatori» della PIC Systems AG.



» Presso le sedi degli sponsor, gli ospiti ricevono informazioni di prima mano e, al contempo, sono offerte numerose opportunità di networking e confronto con colleghi specializzati e professionisti.

«Fatti e cifre» SPIK 2026



L'apertura delle porte per la **«Mezza giornata CMS» lunedì 16 marzo 2026** è prevista alle ore 12.30. Il programma inizia a partire dalle 13.15. Oltre a un discorso di apertura e a un Keynote, si terranno quattro presentazioni di 45 minuti ciascuna (in due sessioni parallele in due sale). A partire dalle ore 17.00 ci sarà un aperitivo. L'evento si concluderà alle ore 18.00.

L'apertura delle porte per la giornata principale dello SPIK **martedì 17 marzo 2026** è prevista alle ore 07.30. Il programma inizia alle 08.45 con il discorso di benvenuto, seguito da una presentazione plenaria sul tema «droni». A partire dalle ore 10.00, sono previste, in sessioni parallele, 20 presentazioni specialistiche e quattro contributi NEDIK. Queste si terranno in quattro sale. È prevista una pausa pranzo dalle 12.00 alle 13.00. Alle 13.00 avrà luogo la plenaria di mezzogiorno e la seconda parte delle presentazioni inizierà alle 14.00. L'aperitivo a partire dalle ore 16.00 offrirà ancora opportunità di networking. Lo SPIK 2026 chiuderà ufficialmente le porte alle ore 18.00.

Ulteriori **informazioni**, inclusi i dettagli su programma, location e come arrivare, sono reperibili su www.swisspoliceict.ch.

I **biglietti** potranno essere acquistati su: www.eventfrog.ch

Come sempre, i contributi che si concentrano su progetti di approvvigionamento in corso o recentemente completati saranno molto concreti. Tra gli esempi presentati allo SPIK 2026 rientrano l'introduzione del sistema di comunicazione Mico presso la polizia cantonale del Ticino (progetto NOTIS; Supercomputing Systems AG) e la modernizzazione della centrale di emergenza medica dell'organizzazione cantonale di salvataggio vallesana KWRO (HxGN Schweiz AG).

Biglietti e partecipazione

Tutti coloro che desiderano visitare lo SPIK 2026 e/o partecipare alla «mezza giornata CMS» avranno bisogno di un biglietto per ogni giornata di partecipazione (vedi riquadro). Questi sono come sempre a pagamento per i rappresentanti del mondo imprenditoriale e i privati, mentre i membri di autorità, amministrazione, organizzazione a girofaro blu, ecc. potranno beneficiare dell'ingresso gratuito.



AKKUPOINT Finger-PTT mit Direktstecker zu TPH900

- ✓ Direkter Anschluss am Funkgerät
- ✓ Kabellänge 100cm für mehr Bewegungsfreiheit
- ✓ Ideal für diskrete Tragweise
- ✓ Kombinierbar mit unauffälligen Bluetooth-Kopfhörern
- ✓ Unauffällig. Praktisch. Einsatzbereit

Art. Nr. 991738



PTT

AkkuPoint AG | Durisolstrasse 10 | 5612 Villmergen | 043 555 06 66 | info@akkupoint.ch | www.akkupoint.ch

Banknoten im mobilen Einsatz identifizieren und dokumentieren – schnell und sicher

Im FOKUS-Artikel dieser Ausgabe beleuchten wir, wie Identifikationsnummern von Banknoten für ein effizientes Bargeld-Tracking verwendet werden können. Damit das auch im mobilen Einsatz klappt, entwickelt die OVD Kinegram AG aktuell die App «BANKNOTE SCANNER». Diese wird am SPIK 2026 live demonstriert – und es werden noch Institutionen gesucht, die sie im Feldversuch erproben.

Immer wieder stehen Fahndungs-, Ermittlungs- und Strafverfolgungskräfte vor der Aufgabe, Banknoten identifizieren und dokumentieren zu müssen. Steht ihnen dafür kein stationäres Geldzählgerät mit OCR-Technologie (Optical Character Recognition) zur Verfügung, müssen die Einsatzkräfte die Geldscheine händisch sortieren und zählen, ihren Notenwert aufaddieren und die Identifikationsnummern aller Scheine durch Abschreiben dokumentieren. Eine ebenso mühselige wie zeitraubende und zudem fehleranfällige Arbeit – die überdies stets mehrere Kräfte bindet, da nach dem Vier- oder sogar Sechs-Augen-Prinzip vorgegangen werden muss.

» Die Erfassung und Dokumentation inkriminierter Banknoten ist eine zeitaufwendige und fehleranfällige händische Arbeit. Die App «BANKNOTE SCANNER» macht sie einfach, effizient und sicher.

Banknoten mit dem Smartphone erfassen und dokumentieren

Mit dem Ziel, das Beweismittel-Management bei Fällen, in denen Bargeld respektive Banknoten eine zentrale Rolle spielen, zu erleichtern, hat die Sparte «kinegram.digital» der Schweizer OVD Kinegram AG gemeinsam mit Spezialisten der Elephant & Castle IP GmbH den «BANKNOTE SCANNER» entwickelt – eine mobile App zur Identifikation und Dokumentation von Banknoten für das Beweismittel-Management.

«Die iOS-App kann auf Anfrage, analog wie unsere anderen Apps <CHIP VERIFY> und <MOBILE SCAN SDK>, nahtlos an jedes Polizei-Abklärungssystem (z. B. MACS) oder Fallbearbeitungssystem (z. B. myABI) angebunden werden. So können die Einsatzkräfte aufgefundene Banknoten ganz einfach mit dem Dienst-Smartphone scannen – stapelweise, schnell, effizient und sicher», erklärt Stefan Gabriel, Head of Digital Business der OVD Kinegram AG, auf Nachfrage.



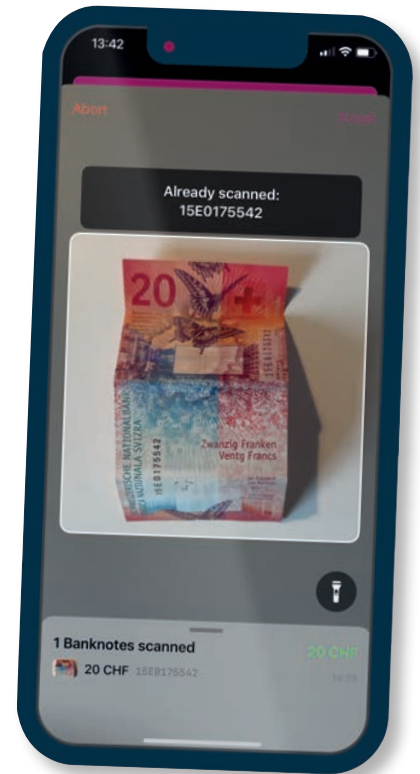
» «BANKNOTE SCANNER»
erkennt die Währung und Notation von Banknoten automatisch,
fotografiert die Scheine und erfasst ihre Identifikationsnummer.

So funktioniert die App «BANKNOTE SCANNER»

Werden die Banknoten mit der App gescannt, identifiziert «BANKNOTE SCANNER» automatisch deren Währung, addiert die Notenwerte, erfasst sämtliche Identifikationsnummern – und macht, zum visuellen Nachweis, Fotos aller Banknoten. So entfällt die bisher bei Bargeldfunden unausweichliche, mühsame und fehleranfällige manuelle Erfassung – sowohl direkt vor Ort als auch im Nachgang bei der Beweismittelverwaltung.

Damit das im mobilen Einsatz jederzeit funktioniert – auch an Orten mit schlechter oder fehlender Mobilfunkabdeckung –, arbeitet die App ohne Online-Verbindung. Auch eine zusätzliche Hardware oder eine gesonderte Software sind nicht erforderlich. Dessen ungeachtet können die erfassten Daten und Bilder natürlich in andere Dienst Anwendungen, etwa das Fallmanagement oder die Asservatenverwaltung, übertragen werden. Dennoch werden, da die Anwendung komplett offline auf dem Diensttelefon läuft, selbst strengste Sicherheits- und Datenschutzanforderungen erfüllt. «In Summe spart die App wertvolle Ressourcen, reduziert Fehler und sorgt für eine nachhaltige Verbesserung der Qualität der Polizeiarbeit», ist Stefan Gabriel überzeugt.

Zu diesem Zweck testen bereits einige Polizeikorps, beispielsweise die Stadtpolizei Zürich, die MVP-Version im Rahmen von Feldversuchen im realen Fronteinsatz. «Die Feedbacks der Testanwender fließen direkt in die finalen Optimierungsschritte ein», verspricht Patrick Brouwer. Daher sucht die OVD Kinegram AG aktuell weitere Institutionen, welche die App im Dienstalltag erproben wollen. «Gemäss unserem Lean-Innovation-Prinzips laden wir Polizeikorps, Zoll- und Grenzwachtkräfte sowie Strafverfolgungsbehörden ein, die MVP-Version von «BANKNOTE SCANNER» in ihrem Berufsalltag zu testen und uns bei der Perfektionierung der Lösung zu unterstützen», betont er.



Testen Sie «BANKNOTE SCANNER» – damit die App perfekt werden kann

Aktuell hat die Entwicklung der App den Status eines «Minimum Value Product» (MVP) erreicht. Das heisst: Die App ist voll funktionsfähig, bietet den Anwendern alle relevanten Kernfunktionen. «Was noch fehlt, ist der finale Feinschliff, damit sie ab dem ersten Tag alle Anforderungen der künftigen Anwender optimal erfüllt», erklärt Patrick Brouwer, Produktspezialist für die App bei der OVD Kinegram AG.

Erleben Sie die App live am SPIK 2026

Interessierte können Patrick Brouwer direkt kontaktieren – oder am SPIK 2026 (siehe separaten Artikel in dieser Ausgabe) auf ihn zukommen. Dort ist die OVD Kinegram AG als Sponsorpartner mit einem Stand (Platz 61) vor Ort. An diesem wird die App live präsentiert – und Interessierte können sich dort oder im Nachgang ebenfalls als Testpartner registrieren.

Mehr Informationen zur «BANKNOTE SCANNER»-App und zu den Feldtests erhalten Interessierte am SPIK 2026 sowie bei Patrick Brouwer von der OVD Kinegram AG, www.kinegram.digital, patrick.brouwer@kinegram.com.



Made in Switzerland.

Tradition löscht kein Chaos!
Digitale Lösungen schon.

Wir zeigen dir wie!

ASmonitor FireHub
Gemeinsam für die digitale Feuerwehr

Identifier et documenter les billets de banque lors d'une intervention mobile, rapidement et en toute sécurité

Dans l'article FOCUS de ce numéro, nous examinons comment les numéros d'identification des billets de banque peuvent être utilisés pour un suivi efficace de l'argent liquide. Pour que ce procédé fonctionne également lors d'interventions mobiles, OVD Kinegram AG développe actuellement l'application « BANKNOTE SCANNER ». Elle sera présentée en direct lors du SPIK 2026. L'entreprise recherche encore des institutions pour la tester sur le terrain.

Les services de recherche, d'enquête et de poursuite pénale ont souvent pour mission d'identifier et de documenter des billets de banque. S'ils ne disposent pas d'un compteur de billets fixe équipé de la technologie OCR (reconnaissance optique de caractères), ils doivent trier et compter les billets à la main, additionner leur valeur faciale et documenter les numéros d'identification de tous les billets en les recopiant. Il s'agit d'un travail fastidieux, source d'erreurs et qui prend du temps, qui mobilise en outre plusieurs agents, car il doit être effectué selon le principe du double ou même du triple contrôle.

» L'enregistrement et la documentation des billets de banque suspects constituent un travail manuel fastidieux et sujet à erreurs. L'application « Banknote Scanner » rend cette tâche simple, efficace et sécurisée.

Saisir et documenter les billets de banque à l'aide d'un smartphone

Pour faciliter la gestion des preuves dans les affaires où l'argent liquide ou les billets de banque jouent un rôle central, la division « kinegram.digital » de l'entreprise suisse OVD Kinegram AG a développé, en collaboration avec les spécialistes d'Elephant & Castle IP GmbH, le « BANKNOTE SCANNER », une application mobile permettant d'identifier et de documenter les billets de banque pour la gestion des preuves.

« Sur demande, l'application iOS peut, comme nos autres applications < CHIP VERIFY > et < MOBILE SCAN SDK >, être connectée de manière fluide à n'importe quel système d'enquête policière (par ex. MACS) ou système de traitement des dossiers (par ex. myABI). Les forces d'intervention

peuvent ainsi scanner très facilement les billets de banque trouvés à l'aide de leur smartphone professionnel, par liasses, rapidement, efficacement et en toute sécurité », explique Stefan Gabriel, responsable des activités numériques chez OVD Kinegram AG, en réponse à notre question.



» L'application « BANKNOTE SCANNER » identifie automatiquement la devise et la valeur des billets de banque, photographie les billets et enregistre leur numéro d'identification.

Voici comment fonctionne l'application « BANKNOTE SCANNER »

Lorsque les billets sont scannés à l'aide de l'application, « BANKNOTE SCANNER » identifie automatiquement leur devise, additionne leur valeur, enregistre tous les numéros d'identification et prend des photos de tous les billets à des fins de preuve visuelle. Cela élimine la saisie manuelle fastidieuse et source d'erreurs qui était jusqu'à présent inévitable lors de la découverte d'argent liquide, tant sur place que lors de la gestion ultérieure des preuves.

Afin de garantir son fonctionnement à tout moment lors d'une intervention mobile, même dans des endroits où la couverture mobile est mauvaise ou inexistante, l'application fonctionne sans connexion Internet. Aucun matériel supplémentaire ni logiciel spécifique n'est nécessaire. Mais les données et les images saisies peuvent bien sûr être transférées vers d'autres applications de service pour la gestion des dossiers ou la gestion des pièces à conviction par exemple. Cependant, comme l'application fonctionne entièrement hors ligne sur le téléphone professionnel, même les exigences les plus strictes en matière de sécurité et de protection des données sont respectées. « Au final, l'application permet d'économiser des ressources précieuses, de réduire les erreurs et d'améliorer durablement la qualité du travail de la police », affirme Stefan Gabriel avec conviction.

Testez « BANKNOTE SCANNER », pour que l'application puisse être perfectionnée

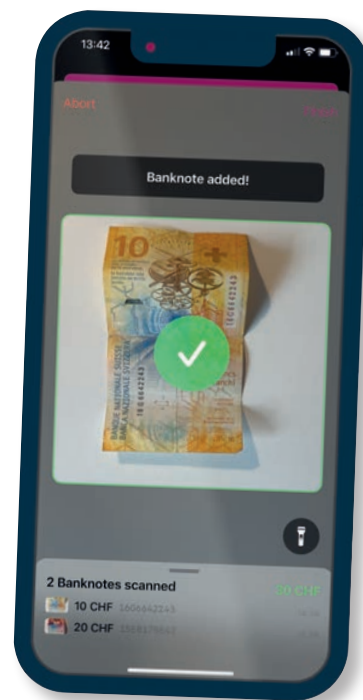
Actuellement, le développement de l'application a atteint le statut de « Produit minimum viable » (MVP). En d'autres termes : L'application est pleinement fonctionnelle et offre aux utilisateurs toutes les fonctionnalités essentielles. « Il ne manque plus que quelques ajustements finaux pour qu'elle réponde de manière optimale à toutes les exigences des futurs utilisateurs dès la première utilisation », explique Patrick Brouwer, spécialiste produit pour l'application chez OVD Kinegram AG.

À cette fin, plusieurs corps de police, dont la police municipale de Zurich, testent déjà la version MVP dans le cadre d'essais sur le terrain en situation réelle. « Les commentaires des utilisateurs testeurs sont directement pris en compte dans les étapes d'optimisation finales », promet Patrick Brouwer. C'est pourquoi OVD Kinegram AG recherche actuellement d'autres institutions souhaitant tester l'application dans leur travail quotidien. « Conformément à notre principe d'innovation lean, nous invitons les corps de police, les douanes, les gardes-frontières et les autorités judiciaires à tester la version MVP de « BANKNOTE SCANNER » dans leur travail quotidien et à nous aider à perfectionner la solution », souligne-t-il.

Découvrez l'application en direct lors du SPIK 2026

Les institutions intéressées peuvent contacter directement Patrick Brouwer ou lui rendre visite au SPIK 2026 (voir l'article séparé dans ce numéro). L'entreprise OVD Kinegram AG y tiendra un stand (emplacement 61) en tant que partenaire sponsor. L'application y sera présentée en direct et les institutions intéressées pourront s'inscrire sur place ou ultérieurement en tant que partenaires de test.

Pour plus d'informations sur l'application « BANKNOTE SCANNER » et les tests sur le terrain, rendez-vous au SPIK 2026 ou contactez Patrick Brouwer de l'entreprise OVD Kinegram AG, www.kinegram.digital, patrick.brouwer@kinegram.com.



Identificare e documentare le banconote nelle operazioni mobili in modo rapido e sicuro

Nell'articolo FOCUS di questo numero chiariamo come servirsi dei numeri identificativi delle banconote per un tracciamento efficiente del contante. Al fine di consentire ciò anche durante le operazioni mobili, OVD Kinegram AG sta sviluppando l'app «BANKNOTE SCANNER». Una dimostrazione live sarà data allo SPIK 2026 e si cercano ancora istituzioni per sperimentazioni sul campo.

Di frequente le forze di indagine, investigazione e dell'ordine hanno il compito di identificare e documentare delle banconote. Se non hanno a disposizione un dispositivo contabanconote fisso con tecnologia OCR (Optical Character Recognition), le forze d'intervento devono ordinare contare le banconote manualmente, sommarne il valore nominale e documentare i numeri identificativi di tutti i biglietti trascrivendoli a mano. Un lavoro stancante e dispendioso, oltre che soggetto a possibili errori, che richiede il coinvolgimento di più operatori, dovendo procedere secondo il principio dei quattro o addirittura dei sei occhi.

» La registrazione e la documentazione di banconote incriminate è un lavoro manuale dispendioso e soggetto ad errori. L'app «Banknote Scanner» lo rende facile, efficiente e sicuro.

Registrare e documentare le banconote con lo smartphone

Al fine di facilitare la gestione delle prove in casi in cui il contante o le banconote hanno un ruolo centrale, la sezione «kinegram.digital» della società svizzera OVD Kinegram AG ha sviluppato, insieme agli specialisti della Elephant & Castle IP GmbH, «BANKNOTE SCANNER», l'app mobile per identificare e documentare le banconote per la gestione delle prove.

«Su richiesta, l'app iOS, analogamente alle nostre altre app <CHIP VERIFY> e <MOBILE SCAN SDK>, può essere perfettamente integrata con qualsiasi sistema investigativo della polizia (ad esempio MACS) o sistema di gestione dei casi (ad esempio myABI). Le forze di intervento possono scansionare le banconote trovate in tutta facilità con lo smartphone di servizio, in pile e in modo rapido, efficiente e sicuro», spiega Stefan Gabriel, Head of Digital Business di OVD Kinegram AG, su nostra richiesta.



» «BANKNOTE SCANNER» riconosce la valuta e il taglio delle banconote in modo automatico, fotografa i biglietti e registra il loro numero identificativo.

Come funziona l'app «BANKNOTE SCANNER»

Quando le banconote vengono scansionate con l'app, «BANKNOTE SCANNER» identifica in modo automatico la valuta, somma i valori nominali, registra tutti i numeri identificativi e, come prova visiva, scatta foto di tutte le banconote. Viene così meno la registrazione manuale adottata sinora al ritrovamento di contanti, dispendiosa, inevitabile e soggetta ad errori, sia in loco sia successivamente durante la gestione delle prove.

Affinché ciò funzioni sempre durante le operazioni mobili, anche in luoghi con copertura mobile scarsa o assente, l'app funziona senza collegamento online. Non occorrono neanche hardware ulteriori o software speciali. Ciononostante, i dati e le immagini rilevati possono essere trasmessi in altre applicazioni di servizio, per la gestione dei casi o delle prove. Inoltre, vengono soddisfatti anche severi requisiti di sicurezza e protezione dei dati, essendo l'applicazione completamente offline sul telefono di servizio. «L'app consente in sintesi un notevole risparmio di risorse, riduce gli errori e garantisce un miglioramento duraturo in termini di qualità nel lavoro di polizia», sostiene Stefan Gabriel con convinzione.

Provare «BANKNOTE SCANNER» per rendere l'app perfetta

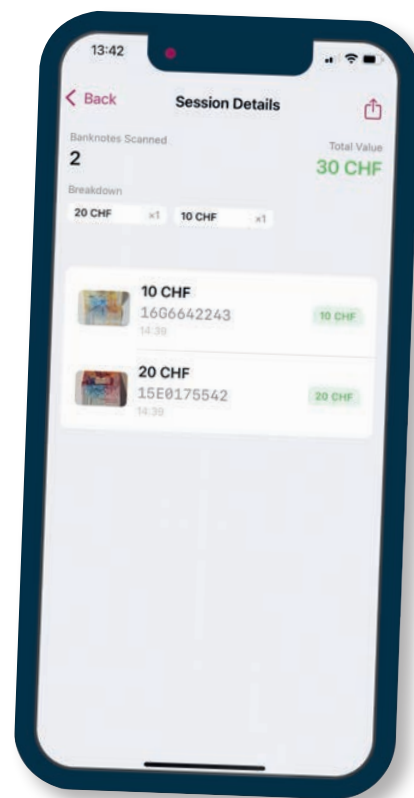
Attualmente, lo sviluppo dell'app ha raggiunto lo stato di «Minimum Value Product» (MVP). Pertanto, l'app è interamente funzionale e offre agli utenti tutte le funzioni centrali rilevanti. «Manca giusto qualche rifinitura, affinché possa soddisfare in modo ottimale tutti i requisiti dei futuri utenti fin dal primo giorno», spiega Patrick Brouwer, specialista di prodotto per l'app di OVD Kinegram AG.

A tal fine, alcuni corpi di polizia, ad esempio la polizia comunale di Zurigo, stanno già testando la versione MVP come parte di sperimentazioni sul campo in situazioni reali di

intervento in prima linea.

«I feedback degli utenti di prova saranno integrati direttamente nelle fasi di ottimizzazione finale», promette Patrick Brouwer. Per questo, OVD Kinegram AG è attualmente alla ricerca di altre istituzioni interessate a testare l'app nel quotidiano di servizio.

«Secondo il nostro principio di innovazione lean, invitiamo i corpi di polizia, le forze doganali e di guardia di frontiera, nonché le forze dell'ordine a testare la versione MVP di «BANKNOTE SCANNER» nel loro quotidiano lavorativo e a sostenerci nel perfezionamento di questa soluzione», sottolinea.



Scoprite l'app live allo SPIK 2026

Gli interessati potranno contattare direttamente Patrick Brouwer o fargli visita allo SPIK 2026 (vedi articolo a parte di questo numero). La OVD Kinegram AG sarà presente con uno stand (posizione 61) in loco in qualità di partner sponsor. In questa occasione, l'app sarà presentata dal vivo e gli interessati potranno registrarsi direttamente lì o successivamente come partner di prova.

Ulteriori informazioni sull'app «BANKNOTE SCANNER» e sulle sperimentazioni sul campo saranno reperibili allo SPIK 2026 o contattando Patrick Brouwer di OVD Kinegram AG, www.kinegram.digital, patrick.brouwer@kinegram.com.

POLIZEITAG HAMBURG
24.03.2026 | EMPIRE RIVERSIDE HOTEL
STÖRUNGSFREI TROTZ HOCHRISIKO:
GEWALTPRÄVENTION UND EINSATZFÜHRUNG BEI FUSSBALLSPIELEN

/om News



Innovative Lösungen für die öffentliche Sicherheit

/om steht für bewährte Lösungen für sämtliche Blaulichtorganisationen. Von der Bussenerfassung über die Parkraumbewirtschaftung bis hin zur Materialverwaltung und Anwendungen für den Zivilschutz. Die zuverlässigen om-Fachapplikationen werden punkto Bedienbarkeit, Optik und Technik unermüdlich weiterentwickelt. Neben der innovativen Software überzeugen wir durch Konstanz in der Servicequalität. Unser Support hilft schnell und unkompliziert.

om FrontRecord – mobile Bussenerfassung. Kontaktlos Übertretungen einkassieren.

om FrontRecord digitalisiert die Erfassung von Übertretungen vollständig und macht manuelle Prozesse überflüssig. Die mobile Lösung für Apple iOS und Android ermöglicht dem Kontrollorgan eine schnelle, sichere und gesetzeskonforme Erfassung direkt vor Ort. Die intuitive Benutzeroberfläche führt die Kontrollperson effizient durch den Prozess und unterstützt sie bei der Schilderkennung mit der eigenentwickelten Lösung **/theia**, die speziell auf CH-Fahrzeugschilder optimiert wurde.

Unmittelbar nach der Erfassung stehen die Daten im **om Bussenportal** zur Verfügung. Dies ermöglicht die Bezahlung,

das Downloaden einer Swiss-QR-Rechnung, die Meldung von Lenkerdaten sowie das Einreichen von Einsprachen. Die zur jeweiligen Ordnungsbusse erstellten Fotos können fallbezogen zur Einsicht freigegeben und zeitlich befristet aufgeschaltet werden.

Ein echter **Gamechanger**: om FrontRecord ermöglicht die sofortige Bezahlung direkt vor Ort, und zwar vollständig integriert in die App. Mit Worldline Tap on Mobile wickeln die Kontrollorgane Zahlungen schnell, kontaktlos und ohne zusätzliches Zahlterminal ganz einfach auf ihrem iPhone oder Android-Gerät ab. Akzeptiert werden die gängigen Zahlungsoptionen wie Visa, Mastercard, TWINT sowie Apple Pay und Google Pay. Mit **Worldline Tap on Mobile** setzen wir auf ein voll integriertes Payment, das neue

Masstäbe für digitale Bezahlprozesse im Schweizer Bussenwesen setzt.

Für die Zuverlässigkeit und wirtschaftliche Effizienz setzt **/om** dabei auf die Partnerschaft mit **Worldline**, einem der führenden Anbieter für bargeldlose Zahlungslösungen. Unsere Kunden profitieren von einer stabilen, bewährten Zahlungsinfrastruktur sowie von ausserordentlich tiefen Kommissionen. Dadurch wird eine nachhaltige Kostenreduktion in der gesamten Zahlungsabwicklung ermöglicht.

Das Ergebnis: kürzere Durchlaufzeiten, höhere Zahlungsmoral, weniger administrativer Aufwand, niedrigere Transaktionskosten und eine moderne, durchgängige Digitalisierung des gesamten Bussenprozesses.

FR om FrontRecord

Busse direkt mit dem Smartphone einkassieren.

Tap on Mobile. Kontaktlos. Ohne Terminal.

/om | WORLDLINE

omcomputer.ch

Künstliche Intelligenz – Segen oder Risiko?

Geht es um moderne Ausrüstung für die Polizei, ist das Thema KI in aller Munde. Doch was leistet KI im Polizeidienst? Was ist erlaubt? Und wie profitieren Kriminelle und Terroristen von KI? Beim Forum Innere Sicherheit 2025 des VSPB in Bern beleuchteten renommierte Fachpersonen diese und weitere Fragen.

«Sicherheit 4.0 – Wie weit kann die Polizei mit KI gehen?» So lautete das Thema des Forums Innere Sicherheit, das der Verband Schweizerischer Polizei-Beamter VSPB Anfang November 2025 in Bern organisierte. Ein Thema, das bewegt, wie ein Blick in den prall gefüllten Forumssaal im Casino Bern zeigte.

KI verändert die Polizeiarbeit nachhaltig

Zum Auftakt des Forums illustrierte Olivier Ribaux, Professor an der Schule für Kriminalwissenschaften der Universität Lausanne, wie rasant die Entwicklungen im Bereich KI voranschreiten und wie stark diese die Politik, die staatlichen Institutionen und die Gesellschaft fordern – und teils überfordern. «KI zwingt uns zu tiefgreifenden Veränderungen und die Polizeikörpers müssen die Entwicklungen, Technologien, Möglichkeiten und Bedrohungen verstehen lernen», erläuterte er.

Dabei greife der alleinige Fokus auf die Frage, was KI für einen selbst leisten kann, zu kurz. «Natürlich sind KI-Apps in vielen Bereichen wie Rapportwesen, Transkription (Sprache zu Text, Bild zu Text), Übersetzung, biometrische Erkennung oder Datenverarbeitung wertvoll. Ebenso zentral ist aber auch die Erkenntnis, dass KI das Wesen von Krimina-

lität verändert», mahnte Olivier Ribaux. «Deshalb wird es nicht genügen, einfach mehr vom Gleichen zu tun. Vielmehr müssen bestehende Strategien und Arbeitsweisen adaptiert werden. Polizeikräfte müssen anders agieren, neue Wege beschreiten, sich an die neuen Gegebenheiten anpassen.»

Neben mehr Forschung zugunsten eines besseren Verständnisses der Integration verschiedener Formen der KI in kriminelle Strukturen, des Potenzials von KI für neue Reaktionsstrategien sowie ihrer weiteren Entwicklung benannte Olivier Ribaux drei Prioritäten für die Schweizer Polizeikörpers: vielfältiges Experimentieren mit diversen KI-Apps, um deren Potenziale und Nutzen zu eruieren. Das Ziehen der richtigen Lehren zugunsten einer zielgerichteten Entwicklung. Und eine Adaption der Rekrutierungs- und Ausbildungsprozesse. «KI erfordert eine andere Polizeiarbeit – und damit auch andere Stellenprofile», so Olivier Ribaux.

Zudem sei es wichtig, die Bevölkerung zu schulen, aufzuklären und mitzunehmen. «Scamming betrifft aktuell vor allem die ältere Generation, welche im Umgang mit digitalen Methoden wie E-Banking oder Online-Shopping (noch) nicht so bewandert ist. Will man die Kriminalität in diesem Bereich eindämmen, ist Aufklärung unerlässlich», betonte Olivier Ribaux.

» Das Forum Innere Sicherheit des VSPB in Bern war einmal mehr aufschlussreich und hervorragend besucht.





» Dr. Jean-Marc Rickli machte klar: Es geht nicht darum, ob, sondern darum wie die Polizei KI künftig nutzen wird. Denn die Gegenseite tut es längst.

Natürlich nutzen längst auch Terroristen KI-Werkzeuge. Deepfake-Videos dienen der Radikalisierung und Rekrutierung, Incels werden mit KI-generierten Inhalten angeworben und – Drohnen mit KI-Gesichtserkennung für gezielte Mordanschläge eingesetzt. Zudem ermöglicht Deep Robotics von Lynx die Entwicklung immer besserer Roboter. «In den USA können Sie auf www.throwflame.com für 9'420 US-Dollar den <Thermonator> kaufen – einen Roboterhund mit Laser-Sicht und einem knapp 30 Meter weit reichenden Flammenwerfer. Stellen Sie sich vor, Sie stehen einem solchen bei einer Hausdurchsuchung im Flur plötzlich gegenüber», warnte Jean-Marc Rickli.

KI macht Kriminalität und Terrorismus schneller, effizienter und bösartiger

Wie stark sich die Methoden Krimineller durch KI bereits verändert haben und weiter verändern werden, zeigte Dr. Jean-Marc Rickli, Head of Global and Emerging Risks des Geneva Centre for Security Policy (GCSP) auf. Er startete mit einem Beispiel, das den Nutzen, aber auch die Risiken von KI sehr konkret macht: «2013 kam mit Google Glass die erste Brille mit integrierter Kamera und Internetverbindung auf den Markt. Zunächst war sie ein Flop. Bis Ray-Ban und Meta das System um eine KI ergänzten. Zwar sind die Möglichkeiten faszinierend. Doch Datenschützer und Sicherheitsexperten schlugen die Hände über dem Kopf zusammen. Denn mithilfe solcher KI-Kamera-Brillen können Kriminelle innert Sekunden alles über eine ihnen zuvor wildfremde Person herausfinden. Damit entfallen auf einen Schlag alle Schutzmechanismen, die wir bisher kannten. Das Resultat ist tiefe Verunsicherung – bei den Menschen wie bei den Polizeikörpern.»

Auch weitere Beispiele von Jean-Marc Rickli sorgten für Raunen im Forum. So liess der Mann, der am Neujahrsmorgen 2025 vor dem Trump Tower in Las Vegas einen Tesla Cybertruck zur Explosion brachte, die dazu benötigte Sprengstoffmenge von einer KI-Lösung berechnen. Andere Kriminelle nutzen die von blauäugigen Eltern auf Social-Media-Plattformen geposteten Bilder und Videos, um deren Sprösslinge in Kinderpornos zu «integrieren». Oder um Schock-Anrufe zu tätigen, bei denen die Opfer mit KI-generierten Stimmen der eigenen Kinder oder Angehörigen konfrontiert werden, um ihnen Geld abzuluchsen. «Eine der führenden Apps zur Erstellung von Deepfakes wurde bereits 134 Millionen Mal heruntergeladen – und selbst der Hersteller weiss nicht, wer sie nutzt», so Jean-Marc Rickli.

All dies, so Rickli, seien erst die Anfänge. «Die Möglichkeiten von KI wachsen exponentiell. Schwarmintelligenz-Systeme für Drohnen und Waffen werden völlig unkontrolliert entwickelt. KI-Systeme, ursprünglich entwickelt für die pharmazeutische Wirkstoffsuche, können so umprogrammiert werden, dass sie tödliche Toxine oder Krankheitserreger entwerfen. In einem Experiment fand eine solche KI in nur einer Stunde vier für eine künstlich erzeugte Pandemie taugliche Viren. Eine andere berechnete in sechs Stunden 40'000 potenzielle C-Waffen. Generative KI-Lösungen ermöglichen zudem ganz neue Arten von Malware. Und die jüngste Evolutionsstufe, die «agentische KI», leitet den Menschen nicht mehr nur an. Sie versteht Fragen, analysiert Lösungswege, entwickelt eigene Strategien – und führt diese auch aus. Hinzu kommen Mensch-Maschine-Schnittstellen. Diese mögen für Menschen mit Handicap ein Segen sein. In den falschen Händen aber werden sie zum unkalkulierbaren Risiko.»

Generell, so Rickli, bestehe die Tendenz, dass KI-Technologien zum unabhängigen Player werden könnten – die sich selbst weiterentwickeln und dabei ganz eigene Strategien verfolgen. «Die Hersteller haben die Kontrolle über die Verwendung ihrer Produkte längst verloren – falls sie diese überhaupt je hatten. Technologie wird immer autonomer, entwickelt sich rasant und teils unkontrolliert. Einst dazu angedacht, die Sicherheit zu stärken, verschärft KI bestehende Gefahren – und generiert teils ganz neuartige Risiken. Hinzu kommt: KI verspricht enorme Gewinne, China und die USA ringen vehement um die Vorherrschaft. Werte wie Ethik, Sicherheit oder Menschlichkeit spielen längst keine Rolle mehr – und die Gesetzgebung hinkt der Entwicklung markant hinterher.»

Rechtliche Leitplanken für KI sind unverzichtbar

Dies gilt auch für die Schweiz, wie Martina Arioli, Rechtsanwältin aus Zürich, aufzeigte. «Die Gesetzeslage ist alles andere als klar. Sowohl hinsichtlich der Verhinderung des Missbrauchs respektive der kriminell motivierten Nutzung von KI als auch bezüglich der Fragen, ob, wozu, unter welcher Voraussetzung und in welchem Rechtsrahmen Polizeikörpers KI-Tools einsetzen dürfen, gibt es grosse Rechtsunsicherheiten», bemängelte Martina Arioli. Zwar werde die Schweiz die KI-Konvention des Europarats, die vor allem die völkerrechtliche Ebene betrifft, ratifizieren und diese sektorbezogen ins Schweizer Recht überführen. Der «EU AI Act» allerdings, also die für alle Mitgliedsstaaten angedachte, direkt anwendbare Verordnung, wird nicht übernommen.

«Der Bund verfügt aktuell nicht über die Kompetenz, den kantonalen KI-Einsatz – beispielsweise in den Polizeikörpers – direkt zu regeln. Dies führt zu Rechtsunsicherheiten auf kantonomer Ebene. Denn wie sollen die Kantone den KI-Einsatz autonom regeln, nicht wissend, wie weit die Revisionen auf Bundesebene reichen werden?», so die Rechtsanwältin. Dabei hat nicht zuletzt der Entscheid zum Luzerner Polizeigesetz vom 17. Oktober 2024 deutlich gemacht, dass KI-gestützte Überwachungsmaßnahmen wie automatisierte Fahrzeugfahndung und Gesichtserkennung nur mit hinreichend bestimmter gesetzlicher Grundlage zulässig sind. Das bedeutet: Die Kantone müssen präzise Regelungen bezüglich Zweckbindung, Speicherfristen und Kontrollmechanismen treffen und den Einsatz von KI differenziert, transparent und grundrechtskonform ausgestalten. Doch man fragt sich, wie die Kantone entsprechende Grundlagen schaffen sollen, wenn dazu kein landesweit anerkannter Rahmen definiert ist.

Ohne ins juristische Detail zu gehen, bleibt die Erkenntnis: KI-Technologien entwickeln sich mit Lichtgeschwindigkeit und Kriminelle sowie Terroristen machen sich deren Fähigkeiten verstärkt zunutze. Ihnen gegenüber stehen Strafverfolgungsbehörden, die für jedwede Nutzung von KI zur Prävention rechtsstaatlicher Gefährdungen klare gesetzliche Grundlagen zu respektieren haben – welche bislang noch weitgehend inexistent sind. Das ist erschreckend und wird sicher nicht dazu beitragen, dass aus der tiefgreifenden Verunsicherung, die grosse Teile der Bevölkerung mit Blick auf KI bereits heute empfinden, ein starkes Vertrauen in den Staat und dessen Institutionen erwachsen könnte.

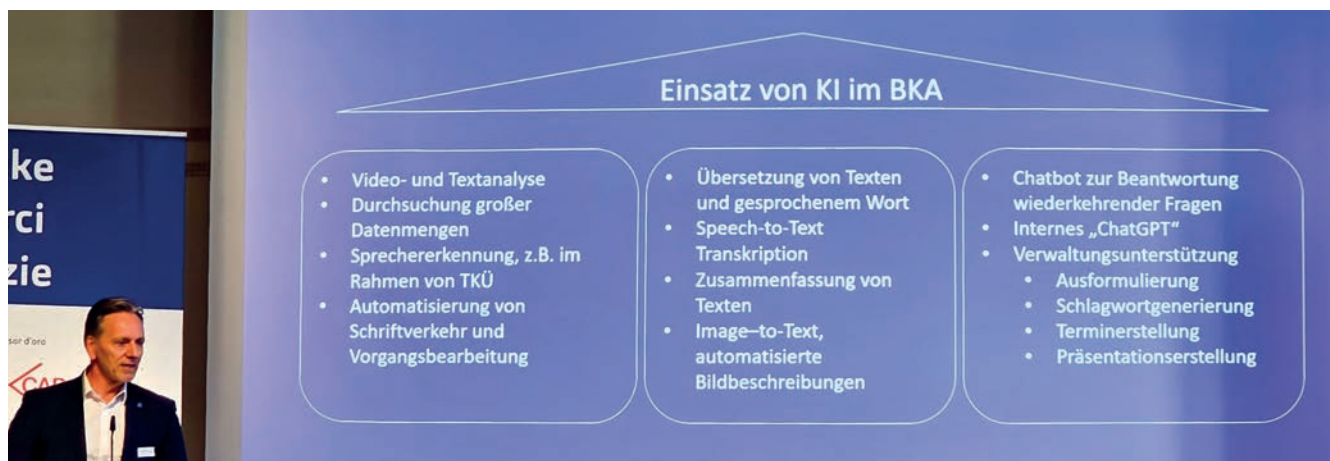
Das deutsche Bundeskriminalamt nutzt KI bereits – mit Erfolg

Dass es auch anders geht, zeigt indes ein Blick über die nördliche Grenze. Dort, beim Deutschen Bundeskriminalamt BKA, wird KI nämlich schon intensiv genutzt, wie BKA-Präsident Holger Münch berichtet: «Seit unserer ersten Nutzung von KI-Tools bei der Aufklärung des <Panama Papers>-Finanzskandals haben wir unsere KI-Kompetenzen kontinuierlich ausgebaut. Aktuell haben wir 65 KI-Systeme im aktiven Betrieb, 15 in der Entwicklung und 25 weitere in unserem KI-Lab in der Anforderungsanalyse. Bei bisher mehr als 7'000 Strafverfahren konnten enorme Mengen Geld und gut 50 Tonnen Rauschgift sichergestellt werden. Zudem wurden gesamthaft mehr als 10'000 Jahre Haftstrafen verhängt. Unsere Gefängnisse sind dank KI proppenvoll.»

Konkret nutzt das BKA einen KI-Chatbot für Anfragen, diverse Transkriptions- und Übersetzungstools sowie Bild- und Videoanalyse-Lösungen samt KI-Gesichtserkennung. Im Zusammenspiel dieser Systeme können BKA-Kräfte nicht nur Gruppenzugehörigkeiten einzelner Krimineller aufdecken, sondern auch komplexe Bandenstrukturen sowie institutionelle Verbindungen erkennen. «Natürlich bedingt dies auch eine intensive Schulung der Mitarbeitenden sowie Veränderungen der personellen Ressourcen», betonte Holger Münch. «Unsere Lichtbildexperten entwickeln sich zu KI-Prozessmanagern, wir bilden keine Bürokräfte mehr aus und beobachten ganz generell eine markante Evolution der Anforderungsprofile. Die Reise geht weg vom Generalisten, hin zum Spezialisten.»

Zudem, so Münch, dürfe man die technologischen Investitionen nicht unterschätzen. «Unser KI-System wächst – und benötigt immer mehr Strom und Rechenleistung. Daher wollen wir im nächsten Schritt eine Multi-Cloud-Architektur realisieren. Hinzu kommen Herausforderungen hinsichtlich Datenmanagement, Compliance und bei der Umsetzung konkreter Use Cases in nutzbare KI-Apps, wozu wir hochqualifizierte Mitarbeitende beschäftigen.»

» BKA-Präsident Holger Münch ist stolz auf das breite Portfolio an KI-Lösungen, die von seiner Institution bereits heute genutzt werden.





» Der «Thermonator» auf Basis eines «Unitree Go2» (China) zeigt, wie leistungsfähig Roboterhunde bereits sind – dank massiver KI-Unterstützung bei der Entwicklung.

Ohne Aus- und Weiterbildung geht es nicht

Sein Tipp an die Schweizer Polizeikörpers lautete: «Zeigen Sie Mut, fangen Sie an mit dem, was Sie dürfen. Schauen, bedenken und diskutieren Sie die Möglichkeiten – und sichern Sie sich die finanziellen Ressourcen für Technologie, Ausbildung und Entwicklung. Zudem müssen Sie klare Anforderungen formulieren, was genau Sie mit der KI tun wollen. Eine Live-Überwachung mit KI-Gesichtserkennung ist ein ganz anderes Szenario, als damit in legal gewonnenem Bildmaterial nach Personen zu suchen, um Täter zu identifizieren oder mögliche Verbindungen zwischen Akteuren krimineller Banden aufzudecken. Je konkreter KI-Nutzungsszenarien definiert werden, desto passgenauer können die dazu nötigen Rechtsgrundlagen definiert werden.»

KI bietet Chancen für die Polizeiarbeit – und die Schweiz muss loslegen

Zustimmung erhielt Holger Münch von Matteo Cocchi, Präsident der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) und Kommandant der Kantonspolizei Tessin. Der sagte: «KI-Instrumente wie prädiktive Kriminalitätsanalyse, automatisierte Überwachungssysteme, Übersetzungs- und Transkriptionshilfen sowie elektronische Ermittlungshilfen steigern Effizienz und Genauigkeit der Ermittlungs- und Präventionsarbeit. Allerdings muss hinter jeder KI-Anwendung ein Mensch stehen. Nur so gewinnen wir das eminent wichtige Vertrauen der Bevölkerung.»

Dabei benennt Matteo Cocchi zwei Herausforderungen: Die Schaffung einer einheitlichen Rechtsgrundlage für den KI-Einsatz bei der Polizei sowie flankierende Massnahmen bei Datenaustausch und -beschaffung. «Aktuell kriege ich Daten aus Deutschland schneller und einfacher als aus Zürich, Genf oder Graubünden. Das muss sich ändern. Zudem müssen wir natürlich sehr darauf achten, dass alle KI-analysierten Daten sicher und verlässlich sind.»

Allen bestehenden Unsicherheiten zum Trotz fordert Matteo Cocchi, dass die Schweiz mächtig aufs Gas drückt. «Wir müssen loslegen – auch auf das Risiko hin, dass der Gesetzgeber uns bei der einen oder anderen Idee zurückpfeifen wird. Denn wer nie losläuft, kann niemals ankommen», mahnte er.

Stefan Aegerter, der am Tag des Forums zugleich seinen letzten Arbeitstag als Direktor des schweizerischen Polizei-Instituts SPI erlebte, sieht wichtige Weichen in der Polizeiausbildung bereits als gestellt an: «Das Bildungspolitische Gesamtkonzept BGK berücksichtigt heute schon diverse durch KI geprägte Zukunftskompetenzen. Polizeikräfte trainieren in KI-Umgebungen und wir wissen, dass KI sinnvoll eingesetzt den Lerneffekt steigert und Ressourcen optimiert.»

Dabei müsse, wie von Matteo Cocchi bereits erwähnt, der Mensch im Zentrum bleiben. «Intuition, Erfahrung und Ethik sind durch keinen Algorithmus ersetzbar. KI soll das Lernen und die Polizeiarbeit erleichtern, nicht den Menschen ersetzen», betonte Aegerter. Zudem sei die Etablierung einer rechtssicheren Balance zwischen Technik und Kontrolle eminent. Künftige Einsatzkräfte müssten für einen verantwortungsvollen Umgang mit Daten, Transparenz und Verhältnismässigkeit sensibilisiert werden.

«Ein grosser Hemmschuh dabei ist der aktuelle Mangel an einheitlichen Rechtsgrundlagen – ohne langwieriges Ping-pong zwischen Bund und Kantonen», sagte Aegerter. «Wir benötigen souveräne Polizeikräfte, die KI verantwortungsbewusst und korrekt nutzen – anhand landesweiter Standards und klar definierter Vorgehensweisen.»

Es gibt viel zu tun – und die Bundesregierung muss handeln

Am Ende eines spannenden Forums wurde deutlich: Die Schweizer Polizei kann sich dem Thema KI nicht entziehen. Zentrale Handlungspunkte sind Investitionen in Entwicklung und Betrieb starker KI-Lösungen, die adäquate Aus- und Weiterbildung der Polizeikräfte sowie die zielgerichtete Evolution des bisher stark auf Generalismus fokussierenden Anforderungsprofils der «uniformierten Sozialarbeiter mit Dienstwaffe», wie der BKA-Präsident Polizeikräfte mit einem Augenzwinkern nennt. Zudem müssen sich Politik und Gesetzgebung zur Decke strecken. Ein KI-Rechtsrahmen ist unverzichtbar, wobei der Bund die Kantone nicht alleinlassen darf. Denn die vom Bundesrat in komplexen Lagen immer wieder zelebrierte Strategie, die «Entwicklungen zu beobachten», wird beim Thema KI krachend scheitern.

L'intelligence artificielle : bénédiction ou risque ?

Lorsqu'il s'agit d'équipements modernes pour la police, le sujet de l'IA est sur toutes les lèvres. Mais quel est le rôle de l'IA dans les services de police ? Qu'est-ce qui est autorisé ? Et comment les criminels et les terroristes tirent-ils profit de l'IA ? Lors du Forum sur la Sécurité intérieure 2025 organisé par la FSFP à Berne, des experts de renom ont abordé ces questions et bien d'autres encore.

« Sécurité 4.0 - Jusqu'où la police peut-elle aller avec l'IA ? » Tel était le thème du Forum sur la Sécurité intérieure organisé début novembre 2025 à Berne par la Fédération suisse des fonctionnaires de police (FSFP). Un sujet qui suscite beaucoup d'intérêt, comme l'a démontré la salle comble du Casino de Berne.

L'IA transforme durablement le travail de la police

En ouverture du Forum, Olivier Ribaux, professeur à l'École des sciences criminelles de l'Université de Lausanne, a illustré la rapidité avec laquelle les développements dans le domaine de l'IA progressent et à quel point ceux-ci sollicitent, et parfois dépassent, la politique, les institutions étatiques et la société. « L'IA nous oblige à opérer des changements profonds et les corps de police doivent apprendre à comprendre les développements, les technologies, les possibilités et les menaces », a-t-il expliqué.

Il ne suffit pas de se concentrer uniquement sur ce que l'IA peut apporter à chacun. « Les applications d'IA sont bien sûr précieuses dans de nombreux domaines tels que la rédaction de rapports, la transcription (de la parole à l'écrit, de l'image à l'écrit), la traduction, la reconnaissance biométrique ou le traitement des données. Mais il est tout

aussi essentiel de reconnaître que l'IA modifie la nature même de la criminalité », a averti Olivier Ribaux. « Intensifier les efforts actuels ne suffira donc pas. Il faudra plutôt adapter les stratégies et les méthodes de travail existantes. Les forces de police doivent agir différemment, explorer de nouvelles voies, s'adapter aux nouvelles circonstances. »

Outre la nécessité d'intensifier la recherche afin de mieux comprendre l'intégration des différentes formes d'IA dans les structures criminelles, le potentiel de l'IA pour de nouvelles stratégies de réaction et son développement futur, Olivier Ribaux a défini trois priorités pour les corps de police suisses : Expérimenter de manière diversifiée différentes applications d'IA afin d'évaluer leur potentiel et leur utilité. Tirer les bonnes leçons afin de favoriser un développement ciblé. Et adapter les processus de recrutement et de formation. « L'IA nécessite un travail policier différent, et donc des profils de poste différents », explique Olivier Ribaux.

Il est également important de former, d'informer et d'impliquer la population. « L'escroquerie touche actuellement principalement la génération plus âgée, qui n'est pas (encore) très familiarisée avec les méthodes numériques telles que les services bancaires en ligne ou les achats en ligne. Si l'on veut endiguer la criminalité dans ce domaine, l'information est indispensable », a souligné Olivier Ribaux.

» Le Forum sur la Sécurité intérieure organisé par la FSFP à Berne a une nouvelle fois été très instructif et a attiré les foules.





» Emmanuel Fivaz, président de la FSFP, a accueilli les participants au Forum par vidéo. « Grâce à l'IA, je parle parfaitement l'allemand et l'italien », a-t-il déclaré en souriant.

L'IA rend la criminalité et le terrorisme plus vifs, plus efficaces et plus malveillants

Le Dr Jean-Marc Rickli, responsable des risques mondiaux et émergents au Centre de politique de sécurité de Genève (GCSP), a montré à quel point les méthodes des criminels avaient déjà changé et continueront de changer grâce à l'IA. Il a commencé par un exemple qui illustre très concrètement les avantages, mais également les risques de l'IA : « En 2013, Google Glass a lancé les premières lunettes avec caméra intégrée et connexion Internet. Le début fut un échec. Jusqu'à ce que Ray-Ban et Meta intègrent l'IA au système. Les possibilités sont certes fascinantes. Mais les défenseurs de la protection des données et les experts en sécurité s'inquiètent. En effet, grâce à ces lunettes équipées d'une caméra et de l'IA, les criminels peuvent découvrir en quelques secondes tout ce qu'il y a à savoir sur une personne qui leur était auparavant totalement inconnue. Tous les mécanismes de protection que nous connaissions jusqu'à présent disparaissent d'un seul coup. Il en résulte une profonde incertitude, tant chez la population que dans les corps de police. »

D'autres exemples cités par Jean-Marc Rickli ont également suscité des réactions lors du Forum. Ainsi, l'individu qui a fait exploser une Tesla Cybertruck devant la Trump Tower à Las Vegas le matin du Nouvel An 2025 a utilisé une solution d'IA pour calculer la quantité d'explosifs nécessaire. D'autres criminels utilisent les photos et vidéos publiées par des parents naïfs sur les réseaux sociaux pour « intégrer » leurs enfants dans des contenus pédopornographiques. Ou pour passer des appels téléphoniques choquants, au cours desquels les victimes sont confrontées à des voix générées par l'IA de leurs propres enfants ou proches afin de leur soutirer de l'argent. « L'une des principales applications permettant de créer des deepfakes a déjà été téléchargée 134 millions de fois, et même son fabricant ignore qui l'utilise », explique Jean-Marc Rickli.

Bien entendu, les terroristes utilisent également depuis longtemps les outils d'IA. Les vidéos deepfake servent à la

radicalisation et à l'enrôlement, les incels sont recrutés à l'aide de contenus générés par l'IA et des drones équipés de la reconnaissance faciale par IA sont utilisés pour des assassinats ciblés. Deep Robotics de Lynx permet en outre de développer des robots toujours plus performants. « Aux États-Unis, vous pouvez acheter sur www.throwflame.com pour 9 420

dollars américains le < Thermonator >, un chien robot doté d'une vision laser et d'un lance-flammes d'une portée de près de 30 mètres. Imaginez que vous vous retrouviez soudainement face à un tel robot lors d'une perquisition dans votre couloir », a averti Jean-Marc Rickli.

Selon lui, tout cela n'est qu'un début. « Les possibilités de l'IA croissent de manière exponentielle. Les systèmes d'intelligence collective pour les drones et les armes sont développés de manière totalement incontrôlée. Les systèmes d'IA, initialement développés pour la recherche de substances pharmaceutiques actives, peuvent être reprogrammés pour concevoir des toxines mortelles ou des agents pathogènes. Dans le cadre d'une expérience, une telle IA a trouvé en seulement une heure quatre virus pouvant être utilisés pour créer une pandémie artificielle. Une autre a calculé en six heures 40 000 armes chimiques potentielles. Les solutions d'IA générative permettent également de créer de tout nouveaux types de logiciels malveillants. Et la dernière étape de l'évolution, l'« IA agentique », ne se contente plus de guider l'homme. Elle comprend les questions, analyse les solutions possibles, développe ses propres stratégies et les met en œuvre. À cela s'ajoutent les interfaces humain-machine. Celles-ci peuvent être une bénédiction pour les personnes en situation de handicap. Mais entre de mauvaises mains, elles deviennent un risque incalculable. »

D'une manière générale, selon Jean-Marc Rickli, les technologies d'IA ont tendance à devenir des acteurs indépendants, qui continuent à se développer et poursuivent leurs propres stratégies. « Les fabricants ont depuis longtemps perdu le contrôle de l'utilisation de leurs produits, s'ils l'ont jamais eu. La technologie devient de plus en plus autonome, elle évolue rapidement et parfois de manière incontrôlée. Initialement conçue pour renforcer la sécurité, l'IA accentue les dangers existants et génère parfois des risques totalement nouveaux. Autre fait : l'IA promet des profits considérables, et la Chine et les États-Unis se disputent avec véhémence la suprématie dans ce domaine. Les valeurs telles que l'éthique, la sécurité ou l'humanité ne jouent plus aucun rôle depuis longtemps, et la législation est nettement à la traîne par rapport à cette évolution. »

Des garde-fous juridiques sont indispensables pour l'IA

Cela vaut également pour la Suisse, comme l'a souligné Martina Arioli, avocate à Zurich. « La situation juridique est tout sauf claire. Il existe une grande incertitude juridique tant concernant la prévention des abus ou de l'utilisation criminelle de l'IA que la question de savoir si, dans quel but, dans quelles conditions et dans quel cadre juridique les forces de police sont autorisées à utiliser des outils d'IA », a déploré Martina Arioli. La Suisse ratifiera certes la convention du Conseil de l'Europe sur l'IA, qui concerne principalement le droit international, et la transposera dans le droit suisse de manière sectorielle. Mais l'« EU AI Act », c'est-à-dire le règlement directement applicable envisagé pour tous les États membres, ne sera pas adopté.

« La Confédération ne dispose actuellement pas de la compétence pour réglementer directement l'utilisation de l'IA au niveau cantonal, par exemple dans les corps de police. Cela entraîne des incertitudes juridiques au niveau cantonal. En effet, comment les cantons peuvent-ils réglementer de manière autonome l'utilisation de l'IA sans savoir jusqu'où iront les révisions au niveau fédéral ? », a déclaré l'avocate. La décision du 17 octobre 2024 relative à la loi sur la police lucernoise a notamment clairement montré que les mesures de surveillance basées sur l'IA, telles que la recherche automatisée de véhicules et la reconnaissance faciale, ne sont autorisées que si elles reposent sur une base légale suffisamment précise. Cela signifie que les cantons doivent établir des réglementations précises concernant l'affectation, les délais de conservation et les mécanismes de contrôle, et concevoir l'utilisation de l'IA de manière différenciée, transparente et conforme aux droits fondamentaux. Mais on peut se demander comment les cantons peuvent créer les bases nécessaires à cet effet si aucun cadre reconnu à l'échelle nationale n'est défini.

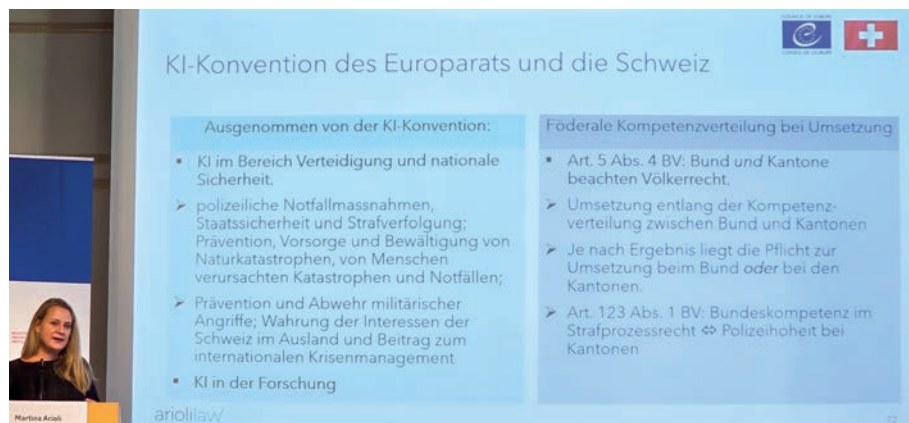
Sans entrer dans les détails juridiques, une chose est sûre : les technologies d'IA se développent à la vitesse de la lumière et les criminels et terroristes exploitent de plus en plus leurs capacités. Face à eux, les autorités judiciaires doivent respecter des bases légales claires pour toute utilisation de l'IA à des fins de prévention des menaces à l'État de droit, bases qui sont encore largement inexistantes à ce jour. Cette situation est effrayante et ne contribuera certainement pas à transformer la profonde incertitude que ressent déjà aujourd'hui une grande partie de la population à l'égard de l'IA en une confiance solide dans l'État et ses institutions.

L'Office fédéral allemand de la police criminelle utilise déjà l'IA, avec succès

Un coup d'œil au-delà de la frontière nord montre toutefois qu'il existe d'autres approches. En effet, l'IA est déjà largement utilisée à l'Office fédéral allemand de la police criminelle (BKA), comme le rapporte son président Holger Münch : « Depuis notre première utilisation d'outils d'IA dans le cadre de l'enquête sur le scandale financier des < Panama Papers >, nous n'avons cessé de développer nos compétences en matière d'IA. Actuellement, nous avons 65 systèmes d'IA en service, 15 en cours de développement et 25 autres en phase d'analyse des besoins dans notre laboratoire d'IA. À ce jour, plus de 7 000 procédures pénales ont permis de saisir d'énormes quantités d'argent et plus de 50 tonnes de stupéfiants. Et plus de 10 000 années de prison ont été prononcées au total. Nos établissements pénitentiaires sont saturés en raison de l'IA. »

Concrètement, le BKA utilise un chatbot IA pour les demandes, divers outils de transcription et de traduction, ainsi que des solutions d'analyse d'images et de vidéos, y compris la reconnaissance faciale par l'IA. Grâce à l'interaction de ces systèmes, les agents du BKA peuvent non seulement découvrir l'appartenance de certains criminels à des groupes, mais également identifier des structures de gangs complexes et des liens institutionnels. « Bien entendu, cela nécessite également une formation intensive des employés et des changements dans les ressources humaines », a souligné Holger Münch. « Nos experts en photographie deviennent des gestionnaires de processus d'IA, nous ne formons plus d'employés de bureau et observons de manière générale une évolution marquée des profils requis. Nous nous éloignons du généraliste pour nous diriger vers le spécialiste. »

Les investissements technologiques ne doivent pas non plus être sous-estimés, selon Holger Münch. « Notre système d'IA se développe et nécessite de plus en plus d'électricité et de puissance de calcul. C'est pourquoi nous souhaitons mettre en place une architecture multi-cloud dans une prochaine étape. À cela s'ajoutent des défis en matière de gestion des données, de conformité et de mise en œuvre de cas d'utilisation concrets dans des applications d'IA exploitables, pour lesquels nous employons du personnel hautement qualifié. »



» L'avocate Martina Arioli a souligné la complexité de la situation juridique actuelle concernant l'utilisation de l'IA par les forces de police suisses.



» Les drones de combat dotés d'une intelligence collective grâce à l'IA ne sont plus une utopie depuis longtemps, et sont également accessibles aux terroristes.

Son conseil aux forces de police suisses est le suivant : « Faites preuve de courage, commencez par ce que vous êtes autorisés à faire. Examinez, réfléchissez et discutez des possibilités, et assurez-vous de disposer des ressources financières nécessaires pour la technologie, la formation et le développement. Vous devez également formuler des exigences claires quant à ce que vous souhaitez accomplir précisément avec l'IA. La surveillance en direct avec la reconnaissance faciale par l'IA est un scénario très différent de la recherche de personnes dans des images obtenues légalement afin d'identifier des auteurs d'infractions ou de découvrir d'éventuels liens entre des membres de bandes criminelles. Plus les scénarios d'utilisation de l'IA sont définis de manière concrète, plus les bases juridiques nécessaires peuvent être définies avec précision. »

L'IA offre des opportunités pour le travail de la police, et la Suisse doit s'y atteler

Holger Münch a reçu l'approbation de Matteo Cocchi, président de la Conférence des commandants des polices cantonales de Suisse (CCPCS) et commandant de la police cantonale du Tessin. Celui-ci a déclaré : « Les outils d'IA tels que l'analyse prédictive de la criminalité, les systèmes de surveillance automatisés, les aides à la traduction et à la transcription ainsi que les aides électroniques à l'enquête améliorent l'efficacité et la précision du travail d'enquête et de prévention. Mais chaque application d'IA doit être supervisée par un être humain. C'est la seule façon de gagner la confiance essentielle de la population. »

Matteo Cocchi identifie deux défis à relever : la création d'une base juridique uniforme pour l'utilisation de l'IA par la police et la mise en place de mesures d'accompagnement pour l'échange et la collecte de données. « Actuellement, j'obtiens plus rapidement et plus facilement des données provenant d'Allemagne que de Zurich, de Genève ou des Grisons. Cela doit changer. De plus, nous devons bien sûr veiller à ce que toutes les données analysées par l'IA soient sûres et fiables. »

Malgré toutes les incertitudes existantes, Matteo Cocchi demande à la Suisse de mettre un coup d'accélérateur. « Nous devons nous lancer, même au risque que le législateur nous rappelle à l'ordre sur l'une ou l'autre idée. Car celui qui ne se lance jamais n'arrivera jamais à destination », a-t-il averti.

La formation initiale et continue est indispensable

Stefan Aegerter, qui a terminé le jour du Forum son dernier jour en tant que directeur de l'Institut suisse de police (ISP), estime que des jalons importants ont déjà été posés dans la formation policière : « Le concept global de politique de formation (CPF) tient déjà compte de diverses compétences d'avenir liées à l'IA. Les forces de police s'entraînent dans des environnements d'IA et nous savons que, utilisée à bon escient, l'IA augmente l'effet d'apprentissage et optimise les ressources. »

Comme l'a déjà mentionné Matteo Cocchi, l'être humain doit rester un pilier important. « L'intuition, l'expérience et l'éthique ne peuvent être remplacées par aucun algorithme. L'IA doit faciliter l'apprentissage et le travail de la police, et non remplacer l'être humain », a souligné Stefan Aegerter. Il est en outre essentiel d'établir un équilibre juridiquement sûr entre la technologie et le contrôle. Les futures forces d'intervention doivent être sensibilisées à l'utilisation responsable des données, à la transparence et à la proportionnalité.

« L'absence actuelle de bases juridiques uniformes, sans va-et-vient fastidieux entre la Confédération et les cantons, constitue un obstacle majeur », a déclaré Stefan Aegerter. « Nous avons besoin de forces de police souveraines qui utilisent l'IA de manière responsable et correcte, sur la base de normes nationales et de procédures clairement définies. »

Il y a beaucoup à faire, et le gouvernement fédéral doit agir

À l'issue d'un forum passionnant, une chose est claire : la police suisse ne peut échapper à l'IA. Les points d'action centraux sont les investissements dans le développement et l'exploitation de solutions d'IA performantes, la formation initiale et continue adéquate des forces de police, ainsi que l'évolution ciblée du profil d'exigences, jusqu'à présent fortement axé sur le généraliste, des « travailleurs sociaux en uniforme portant une arme de service », comme le président de la BKA appelle les forces de police avec un clin d'œil. La politique et la législation doivent en outre se montrer à la hauteur. Un cadre juridique pour l'IA est indispensable, et la Confédération ne doit pas laisser les cantons seuls face à cette question. En effet, la stratégie régulièrement mise en avant par le Conseil fédéral dans les situations complexes, qui consiste à « observer les développements », échouera inmanquablement dans le domaine de l'IA.

Intelligenza artificiale: una benedizione o un rischio?

Quando si parla di attrezzatura moderna per la polizia, il tema IA è sulla bocca di tutti. Ma cosa apporta l'IA al servizio di polizia? Cosa è ammesso? E come beneficiano criminali e terroristi dall'IA? Queste e tante altre domande hanno ricevuto risposta da parte di rinomati esperti al Forum Sicurezza Interna 2025 della FSFP di Berna.

«Sicurezza 4.0 – Fin dove può spingersi la polizia con l'IA?» Questo il tema del Forum Sicurezza Interna organizzato dalla Federazione Svizzera dei Funzionari di Polizia FSFP a inizio novembre 2025 a Berna. Un tema che desta interesse, come dimostra la sala gremita del forum del Casinò di Berna.

L'IA porta cambiamenti di lungo termine nel lavoro della polizia

Olivier Ribaux, professore presso la Facoltà di Criminologia dell'Università di Losanna, ha dato il via al forum, illustrando la rapidità con cui procedono gli sviluppi nel campo dell'intelligenza artificiale e spiegando quanto questi rappresentino una sfida e, a volte, una vera e propria oppressione, per la politica, le istituzioni statali e la società. «L'IA ci costringe ad apportare modifiche profonde e i corpi di polizia devono imparare a comprenderne gli sviluppi, le tecnologie, le possibilità e le minacce», spiega.

Pertanto, non basta chiedersi cosa possa apportare l'IA al singolo. «Certamente le app IA disponibili in vari settori, come reportistica, trascrizione (da parlato a testo, da immagine a testo), traduzione, riconoscimento biometrico o trattamento dei dati sono preziose. Ma è altrettanto impor-

tante comprendere che l'IA modifica la natura stessa della criminalità», avverte Olivier Ribaux. «Pertanto, non basta fare di più nello stesso modo. Occorre adeguare sia le strategie che le modalità di lavoro attuali. Le forze di polizia devono agire diversamente, intraprendere nuove strade, adattarsi alle nuove situazioni.»

Oltre ad una maggiore ricerca per meglio comprendere le modalità di integrazione delle varie forme di IA nelle strutture criminali, il potenziale dell'IA nelle nuove strategie di risposta e l'ulteriore evoluzione di questo strumento, Olivier Ribaux ha indicato tre priorità per i corpi di polizia svizzeri: una sperimentazione varia con diverse app IA per esplorarne potenziale e benefici; trarre le giuste lezioni per incentivare uno sviluppo mirato; un adattamento dei processi di reclutamento e formazione. «L'IA richiede un lavoro differente da parte della polizia» e quindi anche altri profili professionali, continua Olivier Ribaux.

Inoltre, è importante educare la popolazione, informandola e coinvolgendola. «Per ora le truffe interessano soprattutto le vecchie generazioni, (attualmente) meno abili nell'uso di metodi digitali come e-banking o shopping online. Per ridurre la criminalità in questo settore, è indispensabile informare», ha sottolineato Olivier Ribaux.

» Il Forum Sicurezza Interna della FSFP a Berna è stato ancora una volta molto istruttivo e ha visto una grande partecipazione.





» Dalla discussione è emerso che occorre il coraggio di cambiare, serve maggiore cooperazione tra i corpi, casi d'uso concreti, certezza del diritto e, soprattutto, una piattaforma IA per la polizia.

L'IA rende criminalità e terrorismo più rapidi, efficienti e dannosi

Il Dr. Jean-Marc Rickli, Head of Global and Emerging Risks presso il Geneva Centre for Security Policy (GCSP), ha dimostrato quanto l'IA abbia già cambiato e continuerà a cambiare i metodi utilizzati dai criminali. Ha introdotto il discorso con un esempio che rende molto concreto il vantaggio ma anche i rischi dell'IA: «nel 2013, con Google Glass sono arrivati sul mercato i primi occhiali con telecamera integrata e connessione a internet. Inizialmente sono stati un flop. Finché Ray-Ban e Meta non hanno integrato un'IA nel sistema. Le possibilità sono affascinanti. Ma i sostenitori della protezione dei dati e gli esperti di sicurezza alzano le mani inorriditi. Con simili occhiali dotati di telecamera e IA, i criminali possono scoprire qualsiasi cosa su un completo sconosciuto nell'arco di pochi secondi. Pertanto, vengono meno tutti i meccanismi di protezione finora noti. Ne risulta un profondo senso di insicurezza, nelle persone come nei corpi di polizia.»

Anche altri esempi apportati da Jean-Marc Rickli hanno suscitato scalpore nel forum. L'uomo che fece esplodere un Tesla Cybertruck di fronte alla Trump Tower a Las Vegas la mattina di Capodanno del 2025 si era servito di una soluzione IA per calcolare la quantità di esplosivo necessaria. Altri criminali utilizzano le immagini e i video di genitori con occhi blu su piattaforme social media per «integrarne» i figli in siti di pedopornografia. Oppure per fare chiamate shock, in cui le vittime sentono voci di propri figli o familiari, generate dall'IA, a fini di truffa per soldi. «Una delle principali app per creare deepfake è stata scaricata già 134 milioni di volte e nemmeno il produttore sa chi ne usufruisce», afferma Jean-Marc Rickli.

Ovviamente, anche i terroristi usano già da tempo strumenti IA. I video deepfake vengono utilizzati per la radicalizzazione e il reclutamento, gli incel vengono reclutati tramite contenuti generati dall'IA e i droni con riconoscimento facciale basato sull'IA vengono utilizzati per omicidi mirati. Inoltre, Deep Robotics di Lynx permette lo sviluppo di robot sempre

migliori. «Negli USA, su www.throwflame.com, è possibile comprare per 9'420 dollari USA il <Thermonator>, un cane robot con vista laser e un lanciafiamme con una gittata di quasi 30 metri. Immaginate di trovarvi improvvisamente faccia a faccia con qualcosa del genere nel corridoio durante una perquisizione domestica», avverte Jean-Marc Rickli.

Tutto questo è solo l'inizio, continua Rickli. «Le possibilità dell'IA crescono in modo esponenziale. I sistemi di intelligenza collettiva per droni e armi vengono sviluppati in modo del tutto incontrollato. I sistemi IA, originariamente sviluppati per la ricerca di principi attivi farmaceutici, possono essere riconvertiti in modo da progettare tossine o agenti patogeni mortali. In un esperimento, un IA di questo tipo ha trovato in un'ora quattro virus adatti a generare una pandemia creata artificialmente. Un altro ha calcolato 40'000 potenziali armi chimiche in sei ore. Le soluzioni IA generative consentono nuovissimi tipi di Malware. Il più recente stadio evolutivo, l'«IA agente» non funge più solo da guida degli esseri umani. Comprende domande, analizza possibili soluzioni, sviluppa strategie proprie e le esegue. A questo si aggiungono le interfacce uomo-macchina. Queste sono magari una benedizione per i portatori di handicap ma, nelle mani sbagliate, diventano un rischio incalcolabile.

In genere, sostiene Rickli, le tecnologie IA tendono a diventare player indipendenti, che si sviluppano e perseguono strategie proprie. «I produttori hanno perso da tempo il controllo sull'uso dei loro prodotti, se mai ce l'hanno avuto. La tecnologia diventa sempre più autonoma, si sviluppa rapidamente e, in parte, in modo incontrollato. Originariamente pensata per rafforzare la sicurezza, l'IA sta aggravando i pericoli esistenti e, in alcuni casi, generando rischi completamente nuovi. A questo si aggiunge che l'IA promette guadagni enormi e Cina e USA combattono ferocemente per la supremazia. Già da tempo, valori come etica, sicurezza o umanità non giocano più alcun ruolo e la legislazione è notevolmente in ritardo rispetto agli sviluppi.

Delle linee guida legali per l'IA sono indispensabili

Questo vale anche per la Svizzera, come chiarisce Martina Arioli, avvocatessa di Zurigo. «La situazione giuridica è tutt'altro che chiara. Esiste una grande incertezza giuridica sia in termini di prevenzione di abusi o dell'uso criminale dell'IA, sia per questioni relative a se, per quale scopo, in quali condizioni e all'interno di quale quadro giuridico le forze di polizia possano utilizzare strumenti di IA», ha lamentato Martina Arioli. La Svizzera ratificherà la Convenzione sull'IA del Consiglio d'Europa, che riguarda principalmente il livello internazionale, e recepirà questo aspetto settoriale nel diritto svizzero. Non viene però acquisito l'«EU AI Act», ossia il regolamento destinato ad essere direttamente applicabile a tutti gli stati membri.

«Attualmente, la Confederazione non dispone della competenza per regolare l'uso dell'IA a livello cantonale, ad esempio nei corpi di polizia. Questo porta ad insicurezze giuridiche a livello cantonale. Come dovrebbero fare i cantoni a regolare in modo autonomo l'uso dell'IA senza sapere a che punto arriveranno le revisioni a livello federale?», afferma l'avvocata. In particolare, la decisione sulla legge di polizia di Lucerna del 17 ottobre 2024 ha chiarito che le misure di sorveglianza supportate dall'IA, come la perquisizione automatizzata dei veicoli e il riconoscimento facciale, sono ammissibili solo se sussistono basi giuridiche sufficientemente specifiche. In altre parole, i cantoni devono stabilire norme precise in materia di limitazione delle finalità, periodi di conservazione dei dati e meccanismi di controllo, e garantire che l'uso dell'IA sia differenziato, trasparente e conforme ai diritti fondamentali. Tuttavia, ci si chiede come i cantoni possano creare le basi normative necessarie in assenza di un quadro riconosciuto a livello nazionale.

Senza entrare nei dettagli giuridici, si può affermare che le tecnologie IA si stanno sviluppando a una velocità fulminea e criminali e terroristi ne sfruttano sempre di più le capacità. Ad opporsi ci sono le forze dell'ordine, che devono rispettare chiare basi giuridiche per qualsiasi utilizzo dell'IA al fine di prevenire minacce allo stato di diritto, basi ancora in gran parte inesistenti. Questo è un quadro allarmante e non contribuirà certamente a rafforzare la fiducia nello Stato e nelle sue istituzioni, derivante dalla profonda incertezza che ampie fasce della popolazione già provano nei confronti dell'IA.

L'Ufficio Federale della Polizia Criminale Tedesca (Bundeskriminalamt) si serve già con successo dell'intelligenza artificiale.

Che le cose possano essere fatte diversamente lo dimostra uno sguardo oltre il confine settentrionale. Presso l'Ufficio Federale della Polizia Criminale Tedesca (BKA), l'IA è già ampiamente utilizzata, come afferma il Presidente del BKA Holger Münch: «Da quando abbiamo utilizzato per la prima volta strumenti IA nelle indagini sullo scandalo finanziario dei <Panama Papers>, abbiamo costantemente ampliato le nostre competenze in materia di IA. Attualmente disponiamo di 65 sistemi di IA in funzione, 15 in fase di sviluppo e altri 25 nel nostro laboratorio di IA in fase di analisi dei requisiti. In oltre 7'000 procedimenti penali condotti finora, sono state sequestrate ingenti somme di denaro e oltre 50 tonnellate di stupefacenti. Inoltre, sono state comminate condanne a più di 10'000 anni di carcere. Grazie all'IA, le nostre carceri sono sovraffollate.»

In particolare, il BKA utilizza un chatbot basato sull'IA per le indagini, vari strumenti di trascrizione e traduzione, nonché soluzioni di analisi di immagini e video, tra cui il riconoscimento facciale basato sull'IA. L'interazione di questi sistemi consente agli agenti del BKA non solo di scoprire le affiliazioni di gruppo dei singoli criminali, ma anche di identificare complesse strutture di bande e connessioni istituzionali. «Naturalmente, ciò richiede anche una formazione intensiva per i dipendenti e cambiamenti nelle risorse umane», ha sottolineato Holger Münch. «I nostri esperti di fotografia si stanno evolvendo in responsabili di processo basati sull'IA; non formiamo più il personale d'ufficio e, in generale, osserviamo una significativa evoluzione dei requisiti professionali. Il percorso si sta allontanando dai generalisti e si sta spostando verso gli specialisti.»

Inoltre, ha aggiunto Münch, gli investimenti tecnologici non vanno sottovalutati. «Il nostro sistema di intelligenza artificiale sta crescendo e richiede sempre più energia elettrica e potenza di calcolo. Pertanto, il prossimo passo consiste nell'implementazione di un'architettura multi-cloud. A ciò si aggiungono le sfide relative alla gestione dei dati, alla conformità e all'implementazione di casi d'uso concreti nelle app IA utilizzabili, per le quali impieghiamo personale altamente qualificato.»



» Riconvertendo le soluzioni IA per la ricerca medica, i terroristi potrebbero già oggi sviluppare virus in grado di scatenare pandemie o armi biologiche di altro tipo.

GEMEINDE AROSA SUCHT

Infolge Pensionierung des bisherigen Stelleninhabers sucht die Gemeinde Arosa per 1. März 2026 oder nach Vereinbarung **einen Polizisten/eine Polizistin zu 100 Prozent.**

Die Gemeindepolizei ist für die lokale Sicherheit von rund 3'300 Einwohnerinnen und Einwohnern verantwortlich sowie für die Gäste unseres bekannten Tourismusortes.

Wir suchen für unser dreiköpfiges Team einen erfahrenen Polizisten/eine erfahrene Polizistin mit eidg. Fachausweis, welche/r ein abwechslungsreiches Arbeiten im Innen- und Aussendienst schätzt.



Arosa
Gemeinde

Ihre Aufgaben:

- Schalter- und Telefondienst, verwaltungspolizeiliche Aufgaben
- täglicher Kontakt mit verschiedenen Anspruchsgruppen und Kulturen
- Patrouillendienst, verkehrspolizeiliche Aufgaben und Aktionen im fließenden und ruhenden Verkehr
- Ausstellen von Ordnungsbussen
- Sicherheitsdienst, während der Saison Nacht- und Wochenendeinsätze
- verantwortliche Person für BfU- und SIBE-Aufgaben

Ihr Profil:

- abgeschlossene Polizeiausbildung (eidg. FA/Zertifikat)
- hohe Sozialkompetenz, gute Umgangsformen, kommunikatives und freundliches Auftreten
- Teamfähigkeit, Loyalität, Zuverlässigkeit, einwandfreier Leumund sowie psychische und physische Belastbarkeit
- EDV-Kenntnisse
- Fremdsprachen sind von Vorteil
- Führerausweis Kat. B

Wir bieten Ihnen:

- eine verantwortungsvolle, herausfordernde und sinnstiftende Tätigkeit in einem kollegialen und hilfsbereiten Team
- Es erwarten Sie attraktive Arbeitsbedingungen und gute Sozialleistungen.
- Weiterbildungsmöglichkeiten
- Reka-Check, Telefonentschädigung
- Übernahme Risikobeiträge BVG, Wahlsparpläne

Weitere Auskünfte erteilt Ihnen gerne Mathias Buschor, Leiter der öffentlichen Sicherheit, Telefon 081 378 67 17. Ihre Anfrage wird dabei vertraulich behandelt.

Ihre Bewerbung mit den üblichen Unterlagen senden Sie bitte an:

Gemeinde Arosa, Kanzlei Arosa, Rathaus, Poststrasse 168, 7050 Arosa oder an kanzlei@gemeindearosa.ch.

ethelred³

ethelred.ch

Dienstplanungssoftware. Für jede Branche.

Flexibel, dynamisch, anpassungsfähig – so bieten wir mit unserer voll integrierten Dienstplanungssoftware e3 umfangreiche und clevere Lösungen rund um den Personaleinsatz.

**Ferienplanung
im Griff?**
MIT UNSERER WEB-APP
IN EINEM KLICK



Alle forze di polizia svizzere ha rivolto questo consiglio: «Mostrate coraggio, iniziate da ciò che vi è consentito fare. Esaminate, considerate e discutete le possibilità, e assicuratevi le risorse finanziarie per la tecnologia, la formazione e lo sviluppo. Inoltre, dovete formulare requisiti chiari su cosa volete fare esattamente con l'IA. La sorveglianza in tempo reale con il riconoscimento facciale tramite IA è uno scenario completamente diverso rispetto al suo utilizzo per cercare immagini di individui ottenute legalmente al fine di identificare i colpevoli o scoprire potenziali legami tra i membri di bande criminali. Quanto più concretamente vengono definiti gli scenari d'uso dell'IA, tanto più preciso può essere definito il quadro giuridico necessario.»

L'IA offre delle opportunità nel lavoro di polizia e la Svizzera deve darsi una mossa

Holger Münch ha ottenuto il supporto di Matteo Cocchi, Presidente della Conferenza delle comandanti e dei comandanti delle polizie cantonali svizzere (CCPCS) e Comandante della Polizia Cantonale del Ticino. Questi ha affermato: «Strumenti IA come l'analisi predittiva dei reati, i sistemi di sorveglianza automatizzati, gli ausili per la traduzione e la trascrizione e gli strumenti di indagine elettronica aumentano l'efficienza e l'accuratezza del lavoro investigativo e preventivo. Tuttavia, dietro ogni applicazione IA deve esserci un essere umano. Solo in questo modo possiamo guadagnarci la fiducia, di vitale importanza, della popolazione.»

Matteo Cocchi ha individuato due sfide: creare un quadro giuridico uniforme per l'uso dell'IA da parte della polizia, nonché misure di accompagnamento per lo scambio e l'acquisizione dei dati. «Allo stato attuale, è più facile ottenere dati dalla Germania che da Zurigo, Ginevra o Grigioni. Questo deve cambiare. Naturalmente dobbiamo anche prestare la massima attenzione per garantire che tutti i dati analizzati dall'IA siano sicuri e affidabili.»

Ma, nonostante tutte le incertezze esistenti, Matteo Cocchi insiste sul fatto che la Svizzera debba darsi una mossa. «Intanto dobbiamo iniziare, anche a rischio che i legislatori frenino alcune delle nostre idee. Perché si sa che chi si ferma è perduto», ha avvertito.

Senza istruzione e formazione continua non c'è via di scampo

Stefan Aegerter, che proprio in occasione del forum ha vissuto il suo ultimo giorno da Direttore dell'Istituto Svizzero di Polizia (ISP), ritiene che delle decisioni importanti in materia di formazione della polizia siano già state prese: «Il concetto generale di formazione (CGF) incorpora già diverse competenze future plasmate dall'IA. Le forze di polizia si esercitano in ambienti IA e sappiamo che l'IA, se utilizzata in modo appropriato, aumenta l'effetto di apprendimento e ottimizza le risorse.»

Come ha già affermato Matteo Cocchi, l'elemento umano deve rimanere centrale. «Intuizione, esperienza ed etica non possono essere sostituite da alcun algoritmo. L'IA dovrebbe facilitare l'apprendimento e il lavoro di polizia, non sostituire gli esseri umani», ha sottolineato Aegerter. Inoltre, è fonda-



» Per Matteo Cocchi, Presidente della CCPCS e Comandante della Polizia Cantonale del Ticino, una cosa è evidente: «dietro ogni soluzione IA deve esserci un essere umano. Altrimenti perderemo la fiducia della popolazione.»

mentale stabilire un equilibrio giuridicamente solido tra tecnologia e controllo. Le future forze operative devono essere sensibilizzate alla gestione responsabile dei dati, alla trasparenza e alla proporzionalità.

«Un ostacolo importante è l'attuale mancanza di quadri giuridici uniformi, senza lunghi scambi tra Confederazione e Cantoni», ha affermato Aegerter. «Abbiamo bisogno di forze di polizia sovrane che utilizzino l'IA in modo responsabile e corretto, sulla base di standard nazionali e procedure chiaramente definite».

C'è tanto da fare e il governo federale è chiamato ad agire. Al termine di un interessante forum, una cosa è emersa chiaramente: la polizia svizzera non può ignorare la questione dell'IA. I punti chiave d'azione includono investimenti nello sviluppo e nell'utilizzo di soluzioni IA affidabili, una formazione e uno sviluppo professionale adeguati per gli agenti di polizia e l'evoluzione mirata dell'attuale profilo professionale, fortemente generalista, degli «assistenti sociali in uniforme con armi di servizio», come il Presidente del CGF chiama scherzosamente gli agenti di polizia. Inoltre, i responsabili politici e i legislatori devono adottare misure decisive. Un quadro giuridico per l'IA è essenziale e la Confederazione non può lasciare i cantoni soli ad affrontarlo. Perché la classica strategia promossa dal Consiglio federale in situazioni complesse, ossia «osservare gli sviluppi», fallirà miseramente sul tema IA.

Neues zur psychosozialen Notfallversorgung

Der Messerangriff auf einen Angehörigen des Rettungsdienstes Schwyz im November 2025 und die Tragödie von Crans-Montana in der Silvesternacht haben einmal mehr verdeutlicht: Professionelle Hilfe bei belastenden Ereignissen ist enorm wichtig. So erlangt die 12. Fachtagung PSNV am 9. Mai 2026 besonderen Stellenwert.

Wenn etwas Schlimmes passiert, sind sie zur Stelle: die Angehörigen der landesweit tätigen Peer- und Care-Giver-Teams. Sie unterstützen, beraten und begleiten alle Menschen, die durch ein Ereignis betroffen und möglicherweise traumatisiert wurden. Opfer, Angehörige, Augenzeugen und auch die Einsatzkräfte, die am Schadenplatz im Einsatz waren.

Während die hierfür tätigen Fachpersonen – von denen die meisten ehrenamtlich engagiert sind – bei Einsätzen allein oder in kleinen Teams agieren, treffen sie sich einmal im Jahr als «Familie» auf dem Campus Sursee. Denn dort findet jeweils im Frühling mit der Fachtagung PSNV eine der für sie wichtigsten Informations- und Weiterbildungsveranstaltungen statt.

Organisiert wird diese von der Schweizerischen Vereinigung für Psychosoziale Notfallversorgung (SV PSNV) – und am 9. Mai 2026 lädt diese zum 12. Mal zum Treffen auf dem Campus Sursee. Angesprochen werden dabei alle Kräfte der psychologischen und psychosozialen Notfallversorgung, Rettungseinsatzkräfte sowie Mitglieder von Kriseninterventionsteams. Diese erhalten im Rahmen der Tagung wertvolle Inputs für die Erweiterung ihrer persönlichen Fachkompetenzen, aber auch willkommene Möglichkeiten für Vernetzung und den persönlichen Erfahrungsaustausch.

Im Zentrum des eintägigen Anlasses stehen Fachreferate renommierter und erfahrener Einsatzkräfte mit weitreichender Expertise, wobei stets ein breit gefächelter Themenkreis beleuchtet und diskutiert wird. So auch dieses Jahr, in dem fünf spannende Referate auf dem Programm stehen.

» Auf der Fachtagung PSNV in Sursee erfahren Fachpersonen der psychologischen Notfallversorgung, Rettungseinsatzkräfte sowie Mitglieder von Kriseninterventionsteams viel Wissenswertes und Neues.

12. Fachtagung PSNV mit breit gefächertem Programm

Suzanne Martin und André Meier von «Care Kanton Zürich» widmen sich dem Thema «Care-Arbeit bei Kindern und Jugendlichen». Sie präsentieren Erfahrungen und «Lessons Learned» aus diversen Einsätzen und erläutern, welche Anforderungen an die Aus- und Weiterbildung von Care Givern heute gestellt werden.

«Wenn Fragen plagen» lautet das Thema des Referats von Andrea Jutzi, Monika Weiss und Barbara Tiefenauer. Die Spezialistinnen des Nachsorgeangebots «Regio 144 care» beleuchten, wie wichtig es ist, dass Betroffene schwerwiegender Ereignisse Antworten aus erster Hand erhalten, um Geschehenes verstehen und einordnen zu können – und wie dies in der Praxis gelingen kann.

Das Thema «Kindsmisshandlungen und Kinderschutz» steht im Zentrum des Fachreferats von Mischa Oesch, Notfallpsychologin und leitende Psychologin der Kinderschutzgruppe am Inselspital Bern. Sie wird aufzeigen, weshalb Peers und Care Giver wissen sollten, welche Misshandlungsformen es gibt, woran man diese erkennt und weshalb im Umgang mit vernachlässigten oder missbrauchten jungen Menschen eine ergebnisoffene Haltung wichtig ist. Zudem wird sie häufige Fehlannahmen rund um sexuell misshandelte Kinder diskutieren und aufzeigen, weshalb diese so oft schweigen.



Nicht nur Opfer und Angehörige, auch Einsatzkräfte sind Betroffene

Zwei der fünf Referate fokussieren auf von Ereignissen betroffene Einsatzkräfte. Dieter Lenzenhuber, Mitbegründer und Vorstandsmitglied des Traumahilfe-Netzwerks sowie Unterstützer der ARGE Suizidprävention in Bayerisch-Schwaben, Familientherapeut, Traumapädagoge sowie Ausbilder, Einsatzleiter und Verbandsführer in der Notfallrettung, widmet sich dem Thema «Einsatzkräfte nach Gewalterfahrungen – eine Herausforderung unserer Zeit?». Er wird anhand drei konkreter Beispiele (persönliche Gewalterfahrung im Einsatz; Amoktat mit Schusswaffen; Verletzung berufsethischer Prinzipien) unterschiedliche Arten von Gewalterfahrungen darstellen – und die jeweilige Herangehensweise zur Ereignisbearbeitung analysieren.

Dr. Corinna Posingies, promovierte Psychologin und akademische Referentin an der Hochschule Fresenius in Frankfurt a. M., widmet sich den Themen «Selfcare» und «Resilienz». Dabei wird sie nicht nur darlegen, weshalb beides für Einsatzkräfte immer wichtiger wird und weshalb ein mehrdimensionales Verständnis von Resilienz, das Individuen, Teams, Organisationen und Gesellschaft gleichermaßen einbezieht, eminent ist. Sie wird vielmehr den Tagungsgästen praxisnahe Impulse, Übungen und Reflexionsanregungen geben, mit deren Hilfe diese ihre eigene Selbstfürsorge, die Team-Resilienz und ihre professionelle Haltung nachhaltig stärken können.



» Das Miteinander und die Gemeinsamkeit der Aufgaben verleihen der Tagung jeweils eine ganz besondere Atmosphäre.

Tagungsort, Zeitplan und Anmeldung

Die Fachtagung PSNV findet auf dem Campus Sursee bei Luzern statt. Dort bestehen auch Übernachtungsmöglichkeiten. Die Anmeldung erfolgt durch Registration. Diese ist möglich über die Website des Veranstalters (siehe unten). Das Tagesprogramm startet um 9 Uhr mit der Tagungseröffnung durch Corina Bandelli, Präsidentin SV PSNV und Fachperson psychologische Nothilfe NNPN bei der Stiftung Krisenintervention Schweiz (siehe Box), und dauert bis circa 17 Uhr.

Weiterführende Informationen zu Programm, Referaten, Kosten und Anmeldung finden Interessierte auf der Website www.sv-psnv.ch.



» Der ganztägige Anlass dient neben der Wissensvermittlung auch der Vernetzung und dem Erfahrungsaustausch.

«Info»

Stiftung Krisenintervention Schweiz

Die gemeinnützige Stiftung Krisenintervention Schweiz mit Sitz in Winterthur widmet sich der Unterstützung, Beratung und Begleitung traumatisierter Menschen und deren Angehöriger. Mithilfe ihrer hochflexiblen Einsatzorganisation stimmt die Stiftung ihre Arbeit jeweils individuell auf die hilfesuchenden Personen und die Umstände ab, wobei sie ihre Dienstleistungen telefonisch, in ihren eigenen Räumlichkeiten oder am Aufenthaltsort der betroffenen Personen anbietet. Das eingesetzte Team besteht aus Psychologen mit spezieller Ausbildung in Notfallpsychologie, Sozialarbeitenden sowie Fachpersonen der psychologischen Nothilfe NNPN mit Erfahrung im psychosozialen Kriseneinsatz.

Für Blaulichtkräfte bietet die Stiftung Ausbildungen Interessierter zum Peer oder Care Giver sowie praxisnahe Seminare und Workshops zu sämtlichen Themen rund um den Umgang mit schwierigen, belastenden Situationen an. Ergänzend können Peer-Personen von Blaulichtkräften sich im Rahmen von Coachings oder Beratungen mit erfahrenen Peer-Profis austauschen – in schwierigen Fällen, bei der Suche nach Ideen, Strategien und Inputs sowie als Backup-Lösung.

Interessierte Blaulichtinstitutionen erhalten weiterführende Informationen beim Team der Stiftung Krisenintervention Schweiz, www.kriseninterventionschweiz.ch.



» Das Team der Stiftung Krisenintervention Schweiz bietet auch massgeschneiderte Dienstleistungen für Blaulichtkräfte an.

Actualités concernant la prise en charge psychosociale d'urgence

L'agression au couteau d'un membre des services de secours de Schwyz en novembre 2025 et la tragédie de Crans Montana lors de la nuit du Nouvel An ont une nouvelle fois démontré une chose : l'importance cruciale d'une aide professionnelle lors d'événements traumatisants. Le 12^e colloque PSNV, qui se tiendra le 9 mai 2026, revêt donc une importance particulière.

Lorsqu'un événement grave se produit, ils sont immédiatement sur place : les caregivers et les peers actifs dans tout le pays. Ils soutiennent, conseillent et accompagnent toutes les personnes qui ont été touchées et éventuellement traumatisées par un événement. Cela inclut les victimes, les proches, les témoins oculaires et également les services d'urgence qui sont intervenus sur les lieux.

Tandis que les professionnels qui travaillent dans ce domaine, dont la plupart sont bénévoles, agissent seuls ou en petites équipes lors des interventions, ils se réunissent une fois par an en tant que « famille » au Campus Sursee. C'est là que se tient chaque printemps l'un des événements d'information et de formation continue les plus importants pour eux, le Colloque PSNV.

Ce colloque est organisé par la Schweizerische Vereinigung für Psychosoziale Notfallversorgung (SV PSNV - association suisse pour l'aide psychosociale d'urgence) et se tiendra pour la 12^e fois le 9 mai 2026 au Campus Sursee. Il s'adresse à tous les acteurs de l'aide psychologique et psychosociale d'urgence, aux secouristes et aux membres des équipes d'intervention de crise. Dans le cadre de cette conférence, les participants bénéficient d'apports précieux pour élargir leurs compétences professionnelles personnelles, mais également d'occasions bienvenues de réseautage et d'échange d'expériences personnelles.

Des exposés spécialisés présentés par des intervenants renommés et expérimentés possédant une vaste expertise, qui abordent et discutent toujours un large éventail de sujets, sont au cœur de cet événement. C'est également le cas cette année, avec cinq exposés passionnants au programme.

» Lors du colloque PSNV à Sursee, les professionnels de l'aide psychologique d'urgence, les secouristes et les membres des équipes d'intervention de crise acquièrent de nombreuses informations utiles et nouvelles.

12^e colloque PSNV avec un programme varié

Suzanne Martin et André Meier, de « Care Kanton Zürich », abordent le thème du « Travail de soins auprès des enfants et des adolescents ». Ils présentent leurs expériences et les enseignements tirés de diverses interventions et expliquent quelles sont aujourd'hui les exigences en matière de formation initiale et continue des caregivers.

« Lorsque des questions surgissent » était le thème de la présentation d'Andrea Jutzi, Monika Weiss et Barbara Tiefenauer. Les spécialistes du service de suivi « Regio 144 care » soulignent l'importance pour les personnes touchées par des événements graves d'obtenir des réponses de première main afin de pouvoir comprendre et contextualiser ce qui s'est passé, et comment y parvenir dans la pratique.

Le thème « Maltraitance des enfants et protection de l'enfance » est au cœur de la présentation de Mischa Oesch, psychologue d'urgence et psychologue en chef du groupe de protection de l'enfance à l'Inselspital de Berne. Elle expliquera pourquoi les peers et les caregivers doivent connaître les différentes formes de maltraitance, comment les reconnaître et pourquoi il est important d'adopter une attitude ouverte lorsqu'on s'occupe de jeunes négligés ou maltraités. Elle abordera également les idées reçues courantes concernant les enfants victimes d'abus sexuels et expliquera pourquoi ceux-ci gardent si souvent le silence.



Les victimes et leurs proches ne sont pas les seuls concernés, les intervenants le sont également

Deux des cinq exposés se concentrent sur les équipes d'intervention concernées par les événements. Dieter Lenzenhuber, cofondateur et membre du comité directeur du réseau d'aide aux victimes de traumatismes, soutien de la communauté de travail sur la prévention du suicide en Souabe bavaroise, thérapeute familial, pédagogue spécialisé dans les traumatismes, formateur, chef des opérations et responsable des associations dans le domaine des secours d'urgence, aborde le thème « Les forces d'intervention après des expériences de violence : un défi de notre époque ? ». À l'aide de trois exemples concrets (expérience personnelle de la violence lors d'une intervention, fusillade, violation des principes déontologiques), il présentera différents types d'expériences de violence et analysera l'approche pour traiter ces événements.

Le Dr Corinna Posingies, docteure en psychologie et chargée de cours à l'université Fresenius de Francfort-sur-le-Main, abordera les thèmes « Self-care » et « Résilience ». Elle expliquera non seulement pourquoi ces deux aspects sont de plus en plus importants pour les forces d'intervention, mais également pourquoi une compréhension multidimensionnelle de la résilience, qui englobe à la fois les individus, les équipes, les organisations et la société, est essentielle. Elle proposera également aux participants des idées pratiques, des exercices et des pistes de réflexion qui leur permettront de renforcer durablement leur bien-être personnel, la résilience de leur équipe et leur attitude professionnelle.

Lieu, programme et inscription

Le colloque PSNV se tiendra au Campus Sursee, près de Lucerne. Des possibilités d'hébergement y sont également disponibles. Il est nécessaire de s'enregistrer pour s'inscrire. Celui-ci est possible via le site Internet de l'organisateur (voir ci-dessous). Le programme de la journée débutera à 9h avec l'ouverture du colloque par Corina Bandelli, présidente de la SV PSNV et spécialiste en aide psychologique d'urgence NNPN à la fondation Intervention de crise Suisse (voir encadré), et se poursuivra jusqu'à environ 17h.

Les personnes intéressées trouveront de plus amples informations sur le programme, les exposés, les coûts et l'inscription sur le site Internet www.sv-psnv.ch.



» En plus de l'acquisition de connaissances spécialisées, les participants au colloque bénéficient cette année encore d'idées pratiques et d'exercices pour leurs interventions et leur quotidien.



» Outre la transmission de connaissances, cet événement d'une journée est également consacré au réseautage et à l'échange d'expériences.

«Info»

Fondation Intervention de crise Suisse

La fondation d'utilité publique Intervention de crise Suisse, dont le siège se trouve à Winterthur, se consacre au soutien, au conseil et à l'accompagnement des personnes traumatisées et de leurs proches. Grâce à son organisation très flexible, la fondation adapte son travail à chaque personne en demande d'aide et à chaque situation, en proposant ses services par téléphone, dans ses propres locaux ou au domicile des personnes concernées. L'équipe mise en place est composée de psychologues ayant suivi une formation spéciale en psychologie d'urgence, de travailleurs sociaux et de spécialistes de l'aide psychologique d'urgence NNPN ayant une expérience dans les interventions psychosociales en situation de crise.

Pour les services d'urgence, la fondation propose des formations aux personnes intéressées pour devenir peer ou caregiver, ainsi que des séminaires et des ateliers pratiques sur tous les thèmes liés à la gestion de situations difficiles et stressantes. En complément, les peers des services d'urgence peuvent échanger avec des peers professionnels expérimentés dans le cadre de coachings ou de consultations, notamment sur les situations complexes, pour trouver des idées, des stratégies et des contributions, ou encore comme solution de secours.

Les institutions d'urgence intéressées peuvent obtenir de plus amples informations auprès de l'équipe de la fondation Intervention de crise Suisse, www.kriseninterventionschweiz.ch.



» L'équipe de la fondation Intervention de crise Suisse propose également des services sur mesure aux organisations d'urgence.

Nuovi sviluppi nell'aiuto psicosociale d'urgenza

L'aggressione con coltello di un membro del servizio di salvataggio del Canton Svitto a novembre 2025 e la tragedia di Crans Montana nella notte di San Silvestro hanno evidenziato ancora una volta quanto un supporto professionale in caso di eventi stressanti sia di enorme importanza. Ciò conferisce particolare rilevanza al 12. Convegno PSNV del 9 maggio 2026.

Quando accade qualcosa di brutto, ci sono loro: i membri dei Team di Peer e Care Giver nazionali. Essi danno supporto, consigliano e accompagnano tutte le persone che vivono un evento potenzialmente traumatico. Vittime, membri, testimoni oculari e anche le forze di intervento operative sul luogo dell'evento.

Sebbene gli esperti del settore (di cui la maggior parte volontari) operino da soli o in piccole squadre in caso di operazioni, si incontrano una volta all'anno come un'unica «famiglia» presso il Campus Sursee. Infatti, ogni primavera lì si tiene il Convegno PSNV, uno dei loro più importanti eventi informativi e formativi.

Questo viene organizzato dall'Associazione Svizzera per l'aiuto psicosociale d'urgenza (SV PSNV) e il 9 maggio 2026 questa invita alla 12ª edizione dell'incontro al Campus Sursee. Vengono pertanto coinvolte tutte le forze dell'aiuto psicologico e psicosociale d'urgenza, le forze di salvataggio e i membri delle squadre di intervento in caso di crisi. Nell'ambito di un convegno, queste ricevono stimoli preziosi ai fini dell'ampliamento delle loro competenze personali ma anche gradite opportunità di networking e confronto di esperienze.

L'evento, della durata di un giorno, si concentra sulle presentazioni di rinomati esperti delle forze di intervento con una vasta competenza e perciò sarà messa in evidenza e discussa un'ampia gamma di argomenti. Quest'anno saranno al centro del programma cinque interessanti relazioni.

12. Convegno PSNV con programma ben diversificato

Suzanne Martin e André Meier di «Care Canton Zurigo» si dedicano al tema «Lavoro Care con bambini e adolescenti». Presentano esperienze e «lezioni apprese» dalle varie operazioni, illustrando i requisiti oggi necessari per l'istruzione e la formazione dei Care Giver.

«Quando le domande ti tormentano» è stato il tema della presentazione di Andrea Jutzi, Monika Weiss e Barbara Tiefenauer. Gli specialisti del programma di assistenza post-intervento «Regio 144 care» sottolineeranno l'importanza di fornire risposte di prima mano alle persone colpite da eventi gravi per consentir loro di comprendere ed elaborare quanto accaduto, e come questo possa essere conseguito nella pratica.

Il tema «Abuso sui minori e tutela dell'infanzia» sarà al centro della presentazione di Mischa Oesch, psicologa d'urgenza e psicologa responsabile del team di tutela dell'infanzia dell'Inselspital di Berna. Spiegherà perché i Peer e Care Giver dovrebbero conoscere le diverse forme di abuso, come riconoscerle e perché un approccio aperto è fondamentale quando si ha a che fare con giovani trascurati o abusati. Parlerà anche di luoghi comuni sui minori abusati sessualmente e spiegherà perché così spesso rimangono in silenzio.

» Al convegno PSNV di Sursee, gli esperti dell'aiuto psicologico d'urgenza, le forze di salvataggio e i membri delle squadre di intervento in caso di crisi ricevono molte informazioni e scoprono le novità del settore.



Non solo vittime e membri ma anche forze operative

Due delle cinque presentazioni si concentrano sulle forze operative colpite da eventi traumatici. Dieter Lenzenhuber, co-fondatore e membro del consiglio di amministrazione della Rete di assistenza traumatologica e sostenitore della comunità di lavoro per la prevenzione del suicidio nella Svevia Bavarese, terapeuta familiare, educatore e formatore in ambito traumatologico, capo intervento e responsabile di reparto nelle operazioni di salvataggio di emergenza, affronterà il tema «Forze di intervento dopo esperienze di violenza: una sfida del nostro tempo?». Utilizzando tre esempi concreti (esperienza personale di violenza durante un'operazione; una sparatoria; e una violazione dei principi etici professionali), illustrerà diverse tipologie di esperienze traumatiche e analizzerà i rispettivi approcci all'elaborazione di questi eventi.

La Dr. Corinna Posingies, psicologa e consulente accademica presso la Scuola Universitaria Fresenius di Francoforte sul Meno, affronterà i temi del «Selfcare» e della «Resilienza». Non spiegherà solo perché entrambi stanno diventando sempre più importanti per le forze di intervento e perché una comprensione multidimensionale della resilienza, che includa in egual misura individui, team, organizzazioni e società, sia fondamentale ma fornirà ai partecipanti alla conferenza anche spunti pratici, esercizi e stimoli di riflessione, consentendo loro di rafforzare a lungo termine la propria cura di sé, la resilienza del team e l'atteggiamento professionale.

Luogo del convegno, programmazione e iscrizione

Il convegno PSNV si terrà presso il Campus Sursee di Lucerna. Sono previste anche possibilità di pernottamento in loco. È possibile registrarsi per effettuare l'iscrizione. Ciò può essere fatto sul sito web dell'organizzatore (vedi sotto). Il programma inizia alle ore 09.00 con l'apertura del convegno da parte di Corina Bandelli, Presidente di SV PSNV ed esperta di aiuto psicologico d'urgenza RNAPU presso la Fondazione Intervento in Crisi Svizzera (vedi riquadro) e si concluderà verso le ore 17.00.

Ulteriori informazioni su programma, presentazioni, costi e iscrizione sono reperibili sul sito web www.sv-psnv.ch.

» Il team dell'organizzazione renderà anche la 12ª edizione del Convegno PSNV un evento che resterà impresso nella memoria di tutti gli ospiti.



» Presso il luogo dell'evento, il «Campus Sursee», sono disponibili possibilità di pernottamento.

«INFORMAZIONI»

Fondazione Intervento in Crisi Svizzera

La Fondazione Intervento in Crisi Svizzera, senza scopo di lucro e con sede a Winterthur, si dedica al supporto, alla consulenza e all'assistenza di persone traumatizzate e delle loro famiglie. Grazie alla sua struttura operativa altamente flessibile, la fondazione adatta i propri servizi a ogni individuo che richiede aiuto e alle sue specifiche circostanze, offrendo servizi telefonici, presso le proprie strutture o presso la sede della persona interessata. Il team è composto da psicologi con formazione specialistica in psicologia d'urgenza, assistenti sociali e specialisti della Rete Nazionale per l'Aiuto Psicologico d'Urgenza (RNAPU) con esperienza nell'intervento psico-sociale in caso di crisi.

Per le forze a girofaro blu, la fondazione offre corsi di formazione per diventare Peer o Care Giver, nonché seminari e workshop pratici su tutti gli aspetti della gestione di situazioni difficili e stressanti. Inoltre, i Peer delle forze a girofaro blu possono confrontarsi, nell'ambito di coaching o consulenze, in merito a situazioni difficili, ricerca di nuove idee, strategie, stimoli e soluzioni di backup.

Le istituzioni a girofaro blu interessate possono richiedere ulteriori informazioni al team della Fondazione Intervento in Crisi Svizzera, www.kriseninterventionschweiz.ch.



» Corina Bandelli, Presidente PV PSNV, è anche parte del team della Fondazione Intervento in Crisi Svizzera.

» VORSCHAU » APERÇU » ANTEPRIMA

Schwerpunkt Rettung, Schutz und Sicherheit

Im Juni finden gleich zwei internationale Leitmesse statt: die INTERSCHUTZ 2026 in Hannover und die SUISSE PUBLIC 2026 in Bern. Grund genug für uns, die Themenkreise Rettung, Schutz und Sicherheit ins Zentrum der dritten Ausgabe in diesem Jahr zu stellen.

Optimierte Einsatzhygiene
Einsatzkräfte kommen mit allerlei gefährlichen Stoffen in Kontakt. Wir zeigen neue Lösungen für die Einsatzhygiene.

Andere Länder, andere Sitten
Wie und womit arbeiten eigentlich Feuerwehren im benachbarten Ausland – und wäre das auch was für die Schweiz? Wir haben spannende Antworten.

Ausblick und Rückschau
Wir liefern alle Infos zur SUISSE PUBLIC 2026 und einen Überblick, was am SPIK 2026 lief.



Holger de Vries



Holger de Vries



Holger de Vries



SUISSE PUBLIC

» Agenda » Agenda » Agenda

6. bis 7. Mai 2026
DER EUROPÄISCHE
POLIZEIKONGRESS
in Berlin

Alle Infos auf:

www.europaeischer-polizeikongress.de



1. bis 6. Juni 2026
Fachmesse «INTERSCHUTZ»,
Hannover

INTERSCHUTZ

Mehr als 1'300 Aussteller präsentieren Lösungen für Feuerwehr, Rettungswesen, Bevölkerungsschutz, vorbeugenden Brandschutz, Schutzausrüstung sowie Kommunikations- und Leitstellentechnik. Alle Infos auf: www.interschutz.de



16. bis 19. Juni 2026
Fachmesse «SUISSE
PUBLIC»,
Bern

SUISSE
PUBLIC

Die SUISSE PUBLIC nutzt 2026 das gesamte BERNEXPO-Areal – inklusive der neuen Festhalle. Dank der neuen Partnerschaft mit dem Swiss Safety Verband wird die Leitmesse zudem noch interessanter für Angehörige der Blaulichtkräfte. Alle Infos auf: www.suissepublic.ch

» IMPRESSUM » MENTIONS LÉGALES » IMPRONTA

Herausgeber | Editeur | Editore:

blaulicht
| gyrophare bleu | girofaro blu |

Seit 2011 eine eingetragene Marke im eidgenössischen Markenregister

Informationsverlag Schweiz GmbH
Grundstrasse 18, CH-6343 Rotkreuz
Tel.: 041 798 20 60, Fax: 041 798 20 61
E-Mail: office@blaulicht-iv.ch
www.blaulicht-iv.ch

UID-Nummer: CHE-295.811.423

Geschäftsführung | gestion | gestione: Benjamin Kunz

Blaulicht-Verlagsleiter | Directeur éditorial de Blaulicht |
Il direttore editoriale Girofaro Blu: Martin Koller

Chefredakteur | Rédacteur en chef | Caporedattore:
Dr. Jörg Rothweiler

Anzeigenabteilung | Service publicité | Pubblicità Dipartimento:
Franziska Mathys



Titelbild | Photo de couverture
| Foto di copertina:
Anita Fliesser-Steinrisser
Bild: Rega
Gestaltung und Grafik | Création et
graphique | Elaborazione e grafica:
Anita Fliesser-Steinrisser

Index | Indice | Indice:
6113 März 2026

Druck | Pression | pressione: Kromer Print AG / Schweiz

Gesamtauflage | Tirage global | Tiratura:
9'100 Exemplare | exemplaires | copie

Erscheinung | parution | pubblicazione:
6 Mal im Jahr | 6 fois par an | 6 volte all'anno

» Für den Inhalt der diversen Fremddredaktionen übernimmt der Herausgeber keine Haftung. Bei Unterschieden zwischen den verschiedensprachigen Texten bildet jeweils der vom Autor verfasste Originaltext die Referenz. Die Redaktion haftet nicht für Übersetzungsfehler.

» L'éditeur décline toute responsabilité du contenu des différentes rédactions tierces. En cas de différences entre des textes de langues distinctes, le texte original écrit par l'auteur constitue la référence. La rédaction n'est pas responsable des erreurs de traduction.

» L'editore non assume responsabilità per il contenuto delle diverse redazioni esterne. In caso di differenze tra le varie versioni in lingua, prevarrà il testo originale redatto dall'autore. La redazione non risponde di eventuali errori di traduzione.



#AbraxasIntelligence

Abraxas berät und begleitet auch Blaulichtorganisationen dabei, KI zu einem integralen Bestandteil der öffentlichen Verwaltung zu machen.

Abonnieren Sie jetzt den Newsletter für die digitale Schweiz.

abraxas.ch/newsletter


abraxas



Im Notfall zählt jede Sekunde...

POLIZE
BE

POLIZE

BE

zusammen #bereit

Notrufapplikationen und -services
von Swisscom

swisscom

Besuchen Sie uns an der SPIK
in der Festhalle Bern
16. bis 17. März 2026